

# **NEW FRONTIERS IN MARITIME SECURITY: FROM COMPETITION TO COOPERATION**

**Jean-Loup Samaan**

Coordinator

**Máté Szalai**

**Gianmarco Gabriele Marchionna**

**Elaine Donderer**



# **NEW FRONTIERS IN MARITIME SECURITY: FROM COMPETITION TO COOPERATION**

**Jean-Loup Samaan**  
Coordinator

**Máté Szalai**  
**Gianmarco Gabriele Marchionna**  
**Elaine Donderer**

EuroMeSCo has become a benchmark for policy-oriented research on issues related to Euro-Mediterranean cooperation, in particular economic development, security and migration. With 138 affiliated think tanks and institutions and about 700 experts from 32 different countries, the network has developed impactful tools for the benefit of its members and a larger community of stakeholders in the Euro-Mediterranean region.

Through a wide range of publications, surveys, events, training activities, audio-visual materials and a strong footprint on social media, the network reaches thousands of experts, think tankers, researchers, policy-makers and civil society and business stakeholders every year. While doing so, EuroMeSCo is strongly engaged in streamlining genuine joint research involving both European and Southern Mediterranean experts, encouraging exchanges between them and ultimately promoting Euro-Mediterranean integration. All the activities share an overall commitment to fostering youth participation and ensuring gender equality in the Euro-Mediterranean experts' community.

#### POLICY STUDY

Published by the European Institute of the Mediterranean

Academic Peer Reviewer: Anonymous

Editing: Jenny Gilbert

Design layout Maurin.studio

Proofreading Neil Charlton

Layout Núria Esparza

Print ISSN 2938-446X

Digital ISSN 2696-7626

June 2026



The European Institute of the Mediterranean (IEMed), founded in 1989, is a think and do tank specialised in Euro-Mediterranean relations. It provides policy-oriented and evidence-based research underpinned by a genuine Euromed multidimensional and inclusive approach.

The aim of the IEMed, in accordance with the principles of the Euro-Mediterranean Partnership (EMP), the European Neighbourhood Policy (ENP) and the Union for the Mediterranean (UfM), is to stimulate reflection and action that contribute to mutual understanding, exchange and cooperation between the different Mediterranean countries, societies and cultures, and to promote the progressive construction of a space of peace and stability, shared prosperity and dialogue between cultures and civilisations in the Mediterranean.

The IEMed is a consortium comprising the Catalan Government, the Spanish Ministry of Foreign Affairs, European Union and Cooperation, the European Union and Barcelona City Council. It also incorporates civil society through its Board of Trustees and its Advisory Council.

eur@mesco  
Policy Study

# Content

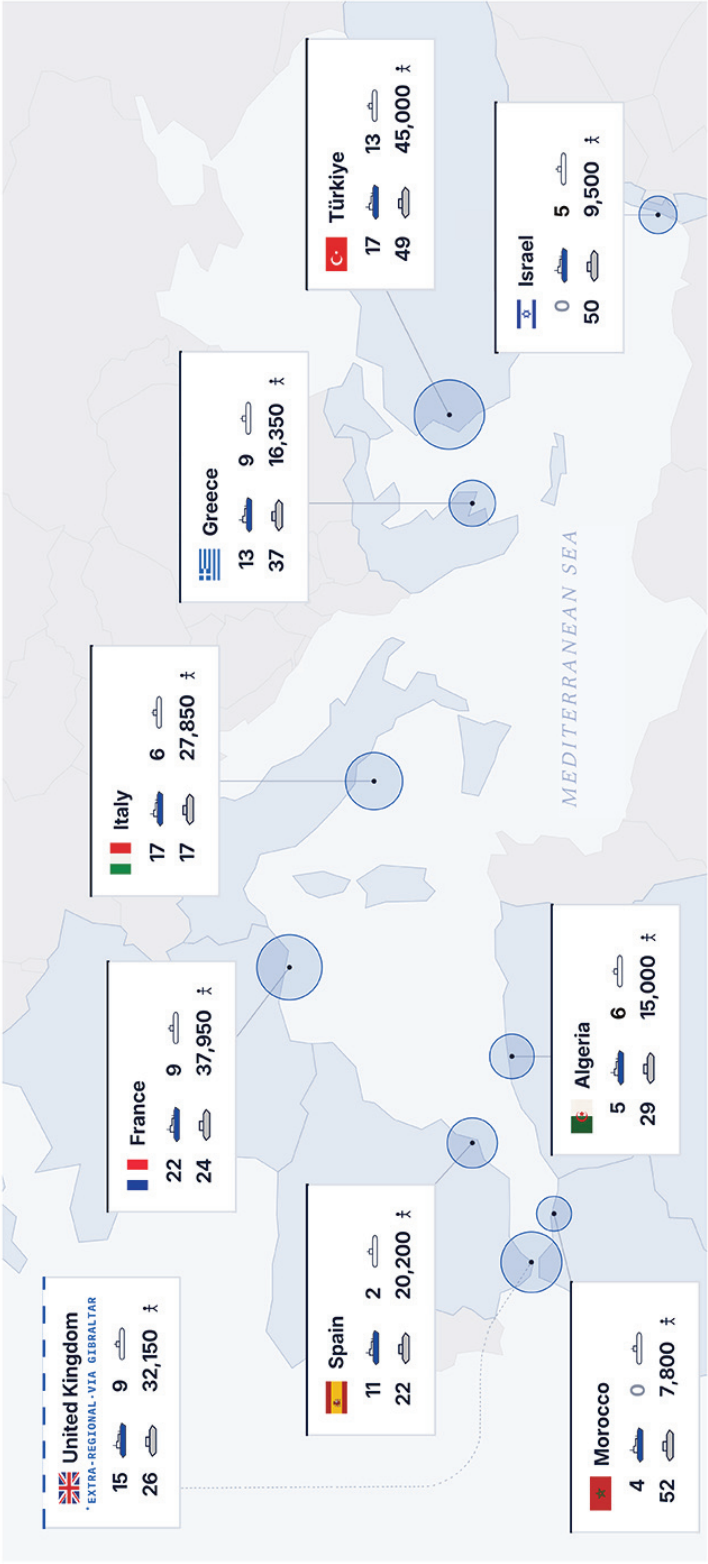
|                                                                                                |           |
|------------------------------------------------------------------------------------------------|-----------|
| <b>List of Acronyms and Abbreviations</b>                                                      | <b>12</b> |
| <b>Introduction</b>                                                                            | <b>16</b> |
| <b>European Navies and the Southern Flank Challenges</b>                                       | <b>22</b> |
| <b>Saudi Emirati Rivalry at Sea and Its Implications for European Interests</b>                | <b>38</b> |
| <b>Keeping the Mediterranean Connected: How Cable Disruptions Can Escalate Maritime Crises</b> | <b>56</b> |
| <b>The Blue Data Bridge: Federated AI for Maritime De-securitisation</b>                       | <b>76</b> |



# Mediterranean naval powers, 2026

Active personnel, principal combatants, submarines and patrol craft.

NEW FRONTIERS IN MARITIME SECURITY:  
FROM COMPETITION TO COOPERATION



SOURCE · IISS, MILITARY BALANCE, 2026  
EUROMESCO · IEMED · 2026



# **List of Acronyms and Abbreviations**

|                   |                                                                                                                                |
|-------------------|--------------------------------------------------------------------------------------------------------------------------------|
| <b>AAE-1</b>      | Asia-Africa-Europe 1 (submarine cable system)                                                                                  |
| <b>AGOR</b>       | Risk-Oriented Gradual Opening (Italian: Apertura Graduata Orientata al Rischio)                                                |
| <b>AI</b>         | Artificial Intelligence                                                                                                        |
| <b>AIS</b>        | Automatic Identification System                                                                                                |
| <b>AIT</b>        | Austrian Institute of Technology                                                                                               |
| <b>API</b>        | Application Programming Interface                                                                                              |
| <b>APT</b>        | Advanced Persistent Threat                                                                                                     |
| <b>AViTeM</b>     | Agency for Sustainable Mediterranean Cities and Territories (French: Agence des villes et territoires méditerranéens durables) |
| <b>BP/RAC</b>     | Blue Plan Regional Activity Centre                                                                                             |
| <b>C4I</b>        | Command, Control, Communications, Computers and Intelligence                                                                   |
| <b>CEF</b>        | Connecting Europe Facility                                                                                                     |
| <b>CER</b>        | Critical Entities Resilience Directive                                                                                         |
| <b>CINEA</b>      | European Climate, Infrastructure and Environment Executive Agency                                                              |
| <b>CISE</b>       | Common Information Sharing Environment                                                                                         |
| <b>CISS</b>       | Center for International and Strategic Studies                                                                                 |
| <b>CMCC</b>       | Euro-Mediterranean Center on Climate Change                                                                                    |
| <b>CMF</b>        | Combined Maritime Forces                                                                                                       |
| <b>COP</b>        | Common Operational Picture                                                                                                     |
| <b>CPMR</b>       | Conference of Peripheral Maritime Regions                                                                                      |
| <b>CRIMARIO</b>   | Critical Maritime Routes Indian Ocean                                                                                          |
| <b>CSD</b>        | Central Ship Database                                                                                                          |
| <b>CTR</b>        | Mutual Transparency Agreement (Italian: Contratto di Trasparenza Reciproca)                                                    |
| <b>DDoS</b>       | Distributed Denial-of-Service                                                                                                  |
| <b>DG MARE</b>    | Directorate-General for Maritime Affairs and Fisheries                                                                         |
| <b>DITTO</b>      | Digital Twin Ocean                                                                                                             |
| <b>EEAS</b>       | European External Action Service                                                                                               |
| <b>EIG</b>        | Europe India Gateway (submarine cable system)                                                                                  |
| <b>EMASOH</b>     | European Maritime Awareness in the Strait of Hormuz                                                                            |
| <b>EMGF</b>       | East Mediterranean Gas Forum                                                                                                   |
| <b>EMODnet</b>    | European Marine Observation and Data Network                                                                                   |
| <b>EMSA</b>       | European Maritime Safety Agency                                                                                                |
| <b>ENISA</b>      | European Union Agency for Cybersecurity                                                                                        |
| <b>EPC</b>        | European Patrol Corvette                                                                                                       |
| <b>ERA</b>        | European Research Area                                                                                                         |
| <b>ETL</b>        | Extract, Transform and Load                                                                                                    |
| <b>EU</b>         | European Union                                                                                                                 |
| <b>EU NAVFOR</b>  |                                                                                                                                |
| <b>/ EUNAVFOR</b> | European Union Naval Force                                                                                                     |
| <b>EUMSS</b>      | European Union Maritime Security Strategy                                                                                      |
| <b>FAIR</b>       | Findable, Accessible, Interoperable and Reusable                                                                               |
| <b>FAO</b>        | Food and Agriculture Organization of the United Nations                                                                        |
| <b>FL</b>         | Federated Learning                                                                                                             |
| <b>FREMM</b>      | European Multi-Mission Frigate (French: Frégate européenne multi-mission)                                                      |
| <b>GAMI</b>       | General Authority for Military Industries                                                                                      |

|                   |                                                                                       |
|-------------------|---------------------------------------------------------------------------------------|
| <b>GCC</b>        | Gulf Cooperation Council                                                              |
| <b>GDPR</b>       | General Data Protection Regulation                                                    |
| <b>GFCM</b>       | General Fisheries Commission for the Mediterranean                                    |
| <b>GPS</b>        | Global Positioning System                                                             |
| <b>gRPC</b>       | gRPC Remote Procedure Calls                                                           |
| <b>HVDC</b>       | High-Voltage Direct Current                                                           |
| <b>ICM-CSIC</b>   | Institute of Marine Sciences, Spanish National Research Council                       |
| <b>ICPC</b>       | International Cable Protection Committee                                              |
| <b>ICZM</b>       | Integrated Coastal Zone Management                                                    |
| <b>IDF</b>        | Israel Defence Forces                                                                 |
| <b>IEMed</b>      | European Institute of the Mediterranean                                               |
| <b>IISS</b>       | International Institute for Strategic Studies                                         |
| <b>IMEWE</b>      | India-Middle East-Western Europe (submarine cable system)                             |
| <b>IMO</b>        | International Maritime Organization                                                   |
| <b>IMS</b>        | Integrated Maritime Services                                                          |
| <b>INFO/RAC</b>   | Information and Communication Regional Activity Centre                                |
| <b>IORIS</b>      | Indo-Pacific Regional Information Sharing                                             |
| <b>IRGC</b>       | Islamic Revolutionary Guard Corps                                                     |
| <b>IRGoY</b>      | Internationally Recognised Government of Yemen                                        |
| <b>IT</b>         | Information Technology                                                                |
| <b>IT/OT</b>      | Information Technology / Operational Technology                                       |
| <b>JERICO-RI</b>  | Joint European Research Infrastructure of Coastal Observatories                       |
| <b>LUISS</b>      | Libera Università Internazionale degli Studi Sociali Guido Carli                      |
| <b>MARPOL</b>     | International Convention for the Prevention of Pollution from Ships                   |
| <b>MCSD</b>       | Mediterranean Commission on Sustainable Development                                   |
| <b>MDA</b>        | Maritime Domain Awareness                                                             |
| <b>MED POL</b>    | Mediterranean Pollution Assessment and Control Programme                              |
| <b>MedECC</b>     | Mediterranean Experts on Climate and Environmental Change                             |
| <b>MEDENER</b>    | Mediterranean Association of National Agencies for Energy Management                  |
| <b>MEDREG</b>     | Association of Mediterranean Energy Regulators                                        |
| <b>MEET</b>       | Mediterranean Experience of Eco-Tourism Network                                       |
| <b>MENA</b>       | Middle East and North Africa                                                          |
| <b>MENBO</b>      | Mediterranean Network of Basin Organisations                                          |
| <b>MIO-ECSDE</b>  | Mediterranean Information Office for Environment, Culture and Sustainable Development |
| <b>MonGOOS</b>    | Mediterranean Oceanographic Network for the Global Ocean Observing System             |
| <b>MPA / MPAs</b> | Marine Protected Area / Marine Protected Areas                                        |
| <b>MSFD</b>       | Marine Strategy Framework Directive                                                   |
| <b>MSSD</b>       | Mediterranean Strategy for Sustainable Development                                    |
| <b>NAPA</b>       | North Adriatic Ports Association                                                      |
| <b>NATO</b>       | North Atlantic Treaty Organization                                                    |
| <b>NCP</b>        | National Collaboration Programme                                                      |
| <b>NGO / NGOs</b> | Non-governmental organization / Non-governmental organizations                        |
| <b>NIS2</b>       | Network and Information Systems Directive 2                                           |
| <b>OME</b>        | Mediterranean Energy Observatory (French: Observatoire Méditerranéen de l'Énergie)    |

|                   |                                                                               |
|-------------------|-------------------------------------------------------------------------------|
| <b>OT</b>         | Operational Technology                                                        |
| <b>P&amp;I</b>    | Protection and Indemnity                                                      |
| <b>PAP/RAC</b>    | Priority Actions Programme Regional Activity Centre                           |
| <b>PCC</b>        | Patrol and Coastal Combatant                                                  |
| <b>PEACE</b>      | Pakistan and East Africa Connecting Europe (submarine cable system)           |
| <b>PIF</b>        | Public Investment Fund                                                        |
| <b>PSC</b>        | Principal Surface Combatant                                                   |
| <b>REMPEC</b>     | Regional Marine Pollution Emergency Response Centre for the Mediterranean Sea |
| <b>RES4MED</b>    | Renewable Energy Solutions for the Mediterranean                              |
| <b>RPC</b>        | Remote Procedure Call                                                         |
| <b>RSF</b>        | Rapid Support Forces                                                          |
| <b>SAF</b>        | Sudanese Armed Forces                                                         |
| <b>SAMI</b>       | Saudi Arabian Military Industries                                             |
| <b>SAR</b>        | Synthetic Aperture Radar                                                      |
| <b>SDG</b>        | Sustainable Development Goal                                                  |
| <b>SIOS</b>       | Svalbard Integrated Arctic Earth Observing System                             |
| <b>SMW4</b>       | South East Asia-Middle East-Western Europe 4 (submarine cable system)         |
| <b>SNEP II</b>    | Saudi Naval Expansion Programme II                                            |
| <b>SOCAT</b>      | Surface Ocean CO <sub>2</sub> Atlas                                           |
| <b>SPA/RAC</b>    | Specially Protected Areas Regional Activity Centre                            |
| <b>SSBN</b>       | Nuclear-powered ballistic missile submarine                                   |
| <b>SSK</b>        | Diesel-electric attack submarine                                              |
| <b>SSN</b>        | Nuclear-powered attack submarine                                              |
| <b>STC</b>        | Southern Transitional Council                                                 |
| <b>TGN</b>        | Tata Global Network                                                           |
| <b>UAE</b>        | United Arab Emirates                                                          |
| <b>UfM</b>        | Union for the Mediterranean                                                   |
| <b>UK</b>         | United Kingdom                                                                |
| <b>UN</b>         | United Nations                                                                |
| <b>UNCLOS</b>     | United Nations Convention on the Law of the Sea                               |
| <b>UNCTAD</b>     | United Nations Conference on Trade and Development                            |
| <b>UNEP/MAP</b>   | United Nations Environment Programme / Mediterranean Action Plan              |
| <b>UNESCO</b>     | United Nations Educational, Scientific and Cultural Organization              |
| <b>UniAdriion</b> | Association of Universities of the Adriatic-Ionian Area                       |
| <b>UNIMED</b>     | Mediterranean Universities Union                                              |
| <b>US</b>         | United States                                                                 |
| <b>VMS</b>        | Vessel Monitoring System                                                      |
| <b>WFP</b>        | World Food Programme                                                          |

# Introduction

**Jean-Loup Samaan**

Senior Research Fellow, Middle East  
Institute of Singapore

From the Russian invasion of Ukraine to the tensions with the United States (US) with administration of President Donald Trump, European countries have faced no choice but to raise their ambitions regarding strategic autonomy - that is, their

ability to protect their interests without relying on an external benefactor (Meijer & Brooks, 2021). As a result, the tone of diplomatic speeches and official white papers across the continent has changed, even as European military expenditures are rising. But for the most part, this re-armament of Europe is driven by a scenario - a confrontation with Russia - that would take place primarily on the territories of the continent. Consequently, maritime issues have remained in the background of most strategic debates.

The scarcity of policy studies on Europe's maritime security matters for several reasons.<sup>1</sup> First, maritime trade remains vital to European economies: in 2024, 75.6% of the European Union (EU)'s imports and 73.7% of its exports by weight transited by sea (Eurostat, 2025). Rail or air transport is nowhere near those figures. As a result, criminal activities or security crises offshore can quickly impact European economies: this was the case when piracy attacks surged off the coast of Somalia in 2008 or, in November 2023, when the Yemen-based Houthis started denying access to the Red Sea to any ship linked to Israel. In both cases, disruptions to maritime trade increased insurance costs for commercial ships and triggered EU military operations (respectively, *Atalanta* and *Aspides*). But whereas the challenge Europe faces on its eastern flank is a classic security issue - i.e., the

possibility of a conflict with Russia - the situation on its southern flank, the area from the Strait of Gibraltar to the Bab el-Mandeb, is more complex.

Europe's southern flank, understood as the political space encompassing the Mediterranean, the Red Sea, and the Persian Gulf, comprises a myriad of littoral states and private actors that collectively shape the security environment. Therefore, Europe's maritime security is not defined by a single challenge but by many of very different natures and scales. For instance, fragile state institutions on the African shores of the Mediterranean can enable criminal or terrorist organisations to build safe havens from which to launch attacks on European interests at sea. Meanwhile, local rivalries, such as those in the East Mediterranean between Greece, Cyprus, and Türkiye, or in the Middle East between Israel and Iran, can quickly escalate into regional conflicts. Moreover, in all these scenarios, governments and international organisations like the EU and North Atlantic Treaty Organization (NATO) are not the only stakeholders. While the human costs of maritime insecurity - including for migrants and coastal communities - fall outside the scope of this study, the security and economic dimensions addressed here have direct consequences for regional stability.

Against that backdrop, this policy report serves three key purposes: to provide a detailed assessment of the threats and challenges facing Europe at sea; to discuss the various roles played by all stakeholders and the ways Europeans can coordinate to better address their maritime security needs; and to offer recommen-

<sup>1</sup> Throughout this study, expressions such as Europe and European countries refer to EU member states, with particular attention to those with a Mediterranean presence. This excludes the United Kingdom (UK) and Türkiye, whose roles are discussed when deemed relevant, in which case they are explicitly mentioned.

dations for policy-makers on how to improve Europe's preparedness in this domain.

To that end, our study group adopted a multidisciplinary approach. Because the challenges facing Europe at sea are multifaceted, so is our report. The four chapters aim to shed light on what we believe to be the four major dimensions of Europe's maritime security:

- 1) *the diplomatic dimension* that defines the type of security arrangements and consultations that Europe as a whole can consider for its maritime security;
- 2) *the military dimension* that revolves around the missions allocated to European armed forces, and particularly its navies, to ensure principles such as freedom of navigation and deterring any attack against Europe from the sea;
- 3) *the economic dimension* that allows us to better grasp the ways instability at sea disrupts European trade and forces its private companies to adapt;
- 4) *the technical dimension* that forces us to consider how maritime security also involves our dependence on sub-sea cables and other infrastructures that can become the target of malign activities.

Methodologically, this policy study employs a mixed qualitative approach, combining several analytical methods across its chapters. Specifically, Chapter 1 draws on a review of open-source defence data - including figures from the IISS Military Balance and EU and NATO operational records - to evaluate the mismatch between security challenges and European naval capacity. Chapter 2 relies on recent policy literature and press sources to ex-

plore the dynamics of the Saudi-Emirati rivalry and its implications for European interests. Chapter 3 builds a threat typology, covers three case studies to analyse escalation pathways, and translates its findings into two practical governance tools. Finally, Chapter 4 uses semi-structured expert interviews with researchers and practitioners, along with a focused literature review, to design a federated Artificial Intelligence (AI) architecture and an accompanying policy roadmap. Taken together, the chapters constitute a coherent whole: analytically distinct but unified by a shared concern with translating findings into actionable recommendations for European maritime governance.

From that perspective, the first chapter by Jean-Loup Samaan covers the strategic environment and its implications for Europe's navies. It explains how the maritime space stretching from the Mediterranean to the Persian Gulf is defined by the co-existence of heterogeneous challenges. On the one hand, security vacuums caused by state fragility or collapse in Libya, Somalia, and Yemen have fuelled non-state criminality such as piracy, illicit trafficking, and irregular migration at sea. Meanwhile, enduring interstate rivalries - between Algeria and Morocco, Greece and Türkiye, Türkiye and Israel, and, most consequentially, between Israel and Iran - feed persistent tensions that can rapidly spill into the maritime domain, as witnessed by the Red Sea crisis in past years or the closure of the Strait of Hormuz most recently.

Amid this surge of challenges, the chapter documents a troubling mismatch. For the past three decades, the capabilities of European navies have steadily declined, and only a few countries (France, Italy, Greece, Spain) retain the ability to project naval power in the southern flank. Consequently, rather than expecting a dramatic

resurgence of national naval investments, the chapter calls for deepening cooperation among European countries and with their partners in North Africa, the Levant, and the Gulf. This could be achieved by strengthening multilateral frameworks at the EU or NATO levels. Minilateral formats such as the 5+5 Dialogue and the East Mediterranean Gas Forum, and joint industrial initiatives such as the European Patrol Corvette project, offer additional avenues to foster cooperation among all the maritime players.

In the second chapter, Máté Szalai investigates the geopolitical rivalry in the Persian Gulf and its impact on Europe's engagement in maritime security. The author underlines how both the tensions between Saudi Arabia and the United Arab Emirates (UAE) and the US-Iran war of 2026 are reshaping maritime security in the Red Sea and the Persian Gulf. Although the Saudi-Emirati rivalry has been building since the late 2010s, it came to the forefront in December 2025 when Saudi Arabia launched air-strikes on UAE-backed forces in Yemen. The intra-Gulf competition now plays out across multiple theatres, most critically in the Horn of Africa, where both states support competing political and military networks. Szalai explains the strategic motives behind the policies of both countries. Specifically, Riyadh pursues a state-centric, risk-averse developmental approach, whereas Abu Dhabi prioritised a more coercive strategy that relies on non-state actors more or less aligned with its ideological agenda. These diverging approaches generate competing webs of partnerships that fight each other, from Sudan to Somalia. Though the Iran war has temporarily de-emphasised the intensity of the Emirati-Saudi dispute, it has not resolved its root causes. In fact, the conflict with Tehran may deepen the divergences. With regard to Europe, the

chapter calls on the EU to formulate a comprehensive Red Sea strategy that outlines its priorities for maritime security and conflict resolution in the area. It also recommends strengthening cooperation with the Gulf Cooperation Council (GCC) as a whole while maintaining neutrality in the Saudi-Emirati competition.

The third chapter, by Gabriele Marchionna, addresses the vulnerability of submarine cable infrastructure to disruption and escalation in the Mediterranean. It shows how the primary risk lies less in physical exposure per se than in the combination of several factors: infrastructure concentration, attribution ambiguity, geopolitical tension, and fragmented governance. Marchionna highlights how technical incidents can acquire geopolitical significance. For instance, the MV Rubymar incident in February 2024, in which the vessel's unsecured anchor severed three major cables during a 13-day drift before sinking, disrupted 25% of telecommunications traffic between Western Asia, North Africa, and Europe. This was not due to a direct attack on digital infrastructure but rather to collateral damage from a Houthi missile strike. From that perspective, the chapter identifies several gaps, such as the absence of an interagency process linking maritime authorities, telecom regulators, cybersecurity agencies, and naval armed forces; jurisdictional ambiguity in operating in international waters; and misaligned priorities between the public and private sectors.

Subsequently, the chapter details two practical tools and three institutional priorities. A minimum resilience baseline could establish common standards for redundancy, continuous monitoring, and repair readiness. Marchionna also presents a 72-hour crisis playbook that provides a decision-making framework for the critical first days after a major disruption. At the

institutional level, the chapter also recommends that NATO strengthen its Maritime Centre for Critical Undersea Infrastructure with a dedicated Mediterranean mandate; that the EU integrate cable incident reporting into its Common Information Sharing Environment; and that the EU and Mediterranean partners use existing formats such as the 5+5 Dialogue and the Union for the Mediterranean (UfM) to establish diplomatic confidence-building measures.

Finally, the fourth chapter, by Elaine Donderer, proposes a technological solution to establish maritime ground truths and shared situational awareness for transnational confidence-building. The chapter starts from an apparent paradox in Mediterranean security: when threats intensify, actors tend to protect national borders by withdrawing operational data from shared Information Technology (IT) systems, inadvertently degrading the collective awareness needed to manage the very threats they face. Building on the EU's existing Common Information Sharing Environment (CISE) and Indo-Pacific Regional Information Sharing (IORIS) infrastructure, the chapter proposes a Mediterranean Federated Learning (FL) architecture - the Blue Data Bridge - that would allow states, private actors, and non-governmental organizations (NGOs) to train shared AI models without ever transferring raw data outside their own servers. The chapter identifies three use cases for shared interests in transboundary waters - shipping accidents, environmental hazards, and climate change

adaptation - in which shared data intelligence would generate a clear common benefit and could serve as entry points for broader maritime cooperation, including among rival states in the Levant and Northern Africa. The chapter then calls on the European Commission and the European Maritime Safety Agency (EMSA) to adopt a Mediterranean Federated Learning pilot architecture using open-source frameworks. It urges the European External Action Service (EEAS) and the UfM to explicitly link environmental monitoring obligations to regional maritime security protocols; Recommendations also include a call on Horizon Europe and the Mediterranean Action Plan of the United Nations Environment Programme (UNEP/MAP) to fund stakeholder engagement and capacity-building and on EU member state transport ministries to devise incentives for private-sector participation. Finally, the European Commission should establish a permanent, cross-sectoral Blue Data Bridge Dialogue Forum to continuously translate federated AI insights into maritime policy and to provide a venue for Track II diplomacy among civil society and private-sector actors across the Mediterranean.

Altogether, the chapters of this policy study call for a revised European approach - one that combines naval cooperation, diplomatic engagement, infrastructure resilience, and a new governance of its data to form a strategy better prepared to deal with the challenges faced in its southern maritime environment.

## References

EUROSTAT. (2025). *Maritime transport dominates international trade*. Eurostat. <https://ec.europa.eu/eurostat/web/products-eurostat-news/w/edn-20250925-1>

MEIJER, H., BROOKS, S. (2021). Illusions of Autonomy Why Europe Cannot Provide for Its Security If the United States Pulls Back. *International Security*, 45(4), 7-43. [https://doi.org/10.1162/isec\\_a\\_00405](https://doi.org/10.1162/isec_a_00405)

# **European Navies and the Southern Flank Challenges**

**Jean-Loup Samaan**

Senior Research Fellow, Middle East  
Institute of Singapore

Assessing Europe's security needs in the maritime space, ranging from the Mediterranean Sea to the Persian Gulf - or, in common military parlance, its «southern flank» - requires us to confront both the types of challenges in the area and the actual European means to address them. More than a mere overview of this geopolitical environment, the first chapter of this policy report highlights two parallel trends that test Europe's ability to secure its interests at sea.

The first is the coexistence of very different security challenges and threats in the maritime space under study. Whereas Europeans face one major challenge on their eastern flank, namely the possibility of a major war with Russia, there is no similar centralising phenomenon on its southern flank. As this first chapter details, Europe's southern maritime security environment is shaped by different, sometimes opposing, trends. Security vacuums in several sub-regions (North Africa, the Horn of Africa, and the Persian Gulf) caused by the collapse of statehoods (respectively in Libya, Somalia, and Yemen) trigger criminal activities at sea, such as piracy and illicit trafficking. At the same time, the region is shaped by the endurance or resurgence of state-to-state rivalries such as those between Algeria and Morocco, Türkiye and Greece, Türkiye and Israel, the United Arab Emirates (UAE) and Saudi Arabia<sup>2</sup> or Israel and Iran. In the first four cases, these disputes often translate into low-intensity tensions, including border skirmishes and naval assertiveness. But in the case of Israel and Iran, the competition has now turned into an open war, first with the 12-day conflict of June 2025 and then more recently with the United States (US)-Israel operation against Iran started in late February 2026.

Amid the myriad challenges facing Europe, a detailed look at how its countries allocate resources to secure their interests reveals a painful reality: the disconnect between worsening security needs and the steady erosion of European navies. Despite a long European tradition of maritime operations, only a few countries on the continent maintain credible fleets capable of rapid deployment in the area. Most recently, the United Kingdom (UK)'s difficulties in quickly dispatching the HMS Dragon destroyer to Cyprus following attacks by Iran underscore the limited capabilities of a navy traditionally considered Europe's most powerful (Boffey, 2026).

Against that backdrop, the chapter first examines the nature of the security issues facing Europe (state rivalries, non-state aggression, illicit trafficking, cyberattacks) and gauges their intensity relative to Europe's interests (existential, major, or peripheral). The second section discusses the operational requirements that follow from the threat estimate. Specifically, the chapter identifies the major limitations regarding the current force structure of European navies. The third part then focuses on the diplomatic implications, examining the foreign policy arrangements that need to be advanced to address those challenges. Specifically, we examine the state of maritime cooperation among European countries (at bilateral and multilateral levels) and with partners in the Mediterranean (North Africa, the Levant) and the Arabian Peninsula.

## A constellation of security challenges

The security environment on Europe's southern flank is characterised by the

<sup>2</sup> The rivalry between Saudi Arabia and the UAE, and its implications for maritime security in the Red Sea and beyond, is the primary focus of Chapter 2 of this study and is therefore not addressed here.

coexistence of distinct challenges that require different means to address them. First is the persistence of internal conflicts in several countries, such as Libya and Yemen. In both cases, years of civil wars have led to the inability of central governments to ensure the monopoly of violence inside their territories. But given their geographic location, both have also let their onshore issues spill over to the off-shore. Since North Atlantic Treaty Organization (NATO)'s operation Unified Protector in 2011, no government in Tripoli has been able to consolidate its authority. As a result, Libya became a gateway for illicit trafficking across the Mediterranean as well as a battlefield for regional competition, with Egypt, Türkiye, Russia, and the UAE playing major roles in fuelling the local disputes (Jacobs, 2020).

State authority in Yemen also collapsed in the early 2010s, as former president Saleh was ousted amid the upheavals of the Arab Spring that spread across the region. Since then, the country has suffered from a bitter war between the Houthis insurgency, aided by Iran, and a flailing government backed by Saudi Arabia. To prevent a full takeover of Yemen by the Houthis, Riyadh launched a major military operation in 2015 that failed to restore order and only aggravated the humanitarian crisis (Juneau, 2024).

The chronic instability in Libya and Yemen cannot be understood as a series of isolated and contained crises. Each of them has had ramifications beyond their neighbourhood. Libya was a key driver in European maritime operations of the 2010s. For instance, Italy's Operation Mare Nostrum, launched in October 2013, and the European Union (EU) Operation Sophia, launched in 2015, aimed to curb the flow of illegal migration (Parente, 2025).

While the security vacuum in areas such as Tripoli and Sanaa contributed to instability at sea, regional competition also hindered collaboration among all stakeholders. In the past decade, Europe's southern flank has been marked by the persistence, if not deterioration, of three major rivalries. First, in North Africa, relations between Algeria and Morocco have steadily worsened since the US recognised Rabat's sovereignty over Western Sahara in December 2020. Algiers severed diplomatic ties with Morocco in August 2021, accusing it of supporting the separatist Kabyle movement and of deepening security ties with Israel against Algeria. The crisis has had economic consequences. The Algerian government closed its airspace to Moroccan aircraft. It also stopped supplying gas to Spain via Morocco as part of the Maghreb-Europe pipeline (Barba, 2022). Since 2025, there have been signs of apparent de-escalation, though the US administration has convened several high-level meetings with delegations from Algeria, Morocco, and the Polisario Front to reach a final agreement on the Western Sahara issue (Henneberg & Medini, 2025). The trajectory of the Algeria-Morocco standoff matters for Europe for several reasons. As a major gas supplier, Algeria retains significant leverage against European countries perceived as too close to Rabat. Furthermore, the rivalry impedes diplomatic efforts at regional governance. Diplomatic instruments such as the 5+5 Dialogue (discussed in greater detail in the third section) have significantly suffered from it.

A further dimension of the Mediterranean security environment is the growing presence of Russia's so-called shadow fleet - vessels operating outside normal regulatory frameworks to circumvent Western sanctions imposed following the invasion of Ukraine. While primarily associated with oil exports in northern European waters, this fleet has expanded its footprint

The chronic instability in Libya and Yemen cannot be understood as a series of isolated and contained crises. Each of them has had ramifications beyond their neighbourhood.

in the Mediterranean, with Libya serving as a key node. Russian-linked vessels have used Libyan ports to facilitate sanctions evasion and logistical support, exploiting the same governance vacuum that enables illicit trafficking more broadly. This represents a direct link between the instability on Europe's eastern flank and the maritime security challenges of the southern flank, and one that European naval and coast guard operations in the area - including EU Operation Irini, whose mandate covers monitoring of the arms embargo - are increasingly called upon to address (Kenner, 2025; Maritime Executive, 2026).

In the Eastern Mediterranean region, the security environment remains defined by the decades-old dispute between Türkiye and Greece. The maritime dimension is central to the tensions between Athens and Ankara as both sides disagree over the delimitation of their territorial waters in the Aegean Sea. According to international maritime law, Greece has the right to extend its territorial waters up to 12 nautical miles (UNCLOS, Section 2, Article 3). However, Türkiye has opposed the claim, arguing that the Greek interpretation severely reduces its own access to the sea. As a result, Greek ambitions in the area, whether in gas exploration or naval deployments, are seen by Ankara as aggressive moves. Since 2006, this has led Türkiye to embrace its so-called Blue Homeland doctrine (*Mavi Vatan*), which directly challenges Greek and Cypriot maritime claims and runs counter to international agreements such as the Treaty of Lausanne and the United Nations Convention on the Law of the Sea (UNCLOS) (Denizeau, 2021). To date, Türkiye is not a signatory to UNCLOS.

The bilateral hostility is also driven by the Cyprus issue. Since gaining independence in 1960, Cyprus has been divided between

Greek and Turkish communities. In 1974, Türkiye's government launched an operation after a coup in Cyprus, supported by the Greek junta at the time. This conflict led to the displacement of both Greek and Turkish populations, and in 1983, a separate Turkish Cypriot state was created - though only recognised by Ankara to this day. Since the failure of United Nations (UN)-led talks in 2017, relations between the two sides have remained tense, making reunification unlikely under the current circumstances (International Crisis Group, 2023).

Over the past 10 years, disagreements between Athens and Ankara have often escalated, with naval displays of force, and Greek officials have criticised what they saw as Türkiye's gunboat diplomacy (Vilhelmsen, 2011). During this period, Türkiye boosted its military spending and made significant investments in its navy: as Table 1 shows, the Turkish navy now has the upper hand over Greece's: its personnel is three times larger, and it operates more platforms across all domains - submarines, patrol and coastal combatants, principal surface combatants. It is also worth noting that the Greek-Turkish standoff often takes the contours of a zero-sum game. In the past decade, third parties such as France and Israel have consistently deepened their military cooperation with Greece (and, to a lesser extent, with Cyprus), while their relations with Türkiye have deteriorated (Samaan, 2016).

Fortunately, since 2023, the Türkiye-Greece conflict has entered a phase of de-escalation, as both nations resumed talks after 16 months without high-level meetings. In December of that year, President Erdogan visited Greece and declared, "We want to turn the Aegean into a sea of peace," signalling a major shift in bilateral relations (Koukantzou & Gumrukcu,

According to international maritime law, Greece has the right to extend its territorial waters up to 12 nautical miles. However, Türkiye has opposed the claim, arguing that the Greek interpretation severely reduces its own access to the sea. As a result, Greek ambitions in the area, whether in gas exploration or naval deployments, are seen by Ankara as aggressive moves.

2023). Although this new diplomatic tone is a positive step, it does not yet mean that all disputes in the eastern Mediterranean have been resolved.

In the meantime, Türkiye's relations with another eastern Mediterranean power, namely Israel, have greatly deteriorated over the past decade. Though governments in Ankara and Jerusalem cultivated close military ties until the mid-2000s, the partnership has suffered several crises since then, starting with the Israeli interception of the Turkish humanitarian flotilla *Mavi Marmara* trying to reach the Gaza Strip in May 2010. The incident led to the death of 10 pro-Palestine activists (including nine Turkish citizens). In the following years, Ankara curbed most of the bilateral cooperation. Then the Gaza war in 2023 led to further Turkish sanctions against Israel, including restrictions on Israeli civilian vessels trading with Türkiye. Since then, tensions between both countries remain high: competing agendas on regional crises like Syria's reconstruction and the Kurdish question fuel regular speculation over the possibility of a conflict (Aydintasbas, 2025).

Lastly, the most consequential regional competition has been between Israel and Iran. Since the 1980s, both countries have faced each other on numerous issues, ranging from Iran's support for Palestinian and Lebanese militias to Tehran's ballistic arsenal and its nuclear programme. After years of indirect confrontation, the tensions turned into a full-scale conflict, first in 2025 during the so-called 12-Day War that saw the Israel Defence Forces (IDF) conducting airstrikes on Iran's nuclear facilities. It then led to another, broader war in late February 2026, which plunged the region into the worst crisis since the US invasion of Iraq in 2003.

Discussing the details of the ongoing conflict between Iran and Israel goes

beyond the scope of this chapter (see Chapter 2 for a detailed account of the war's consequences in the Gulf). But we can here underline its maritime consequences, in particular in the Red Sea and the Strait of Hormuz. Following Hamas's surprise attack on Israel on 7 October 2023, the IDF launched a wide operation against the Gaza Strip that displayed a level of violence unseen before in the Israel-Palestinian conflict. The Gaza War triggered a major crisis in the Red Sea as the Houthis, the aforementioned insurgents, began a campaign of missile and drone attacks against civilian ships crossing the Red Sea. Their stated motive was to express solidarity with Palestinians in the wake of the Gaza War by targeting Israeli vessels, or those headed to or from the country. In reality, many of the ships that were attacked were neither Israeli vessels nor those headed to or from the country (Raydan & Nadimi, 2025). For instance, the first vessel targeted, the *Galaxy Leader*, was Bahamas-flagged, British-owned, and travelled from Turkey to India.

The Houthi campaign directly affected global supply chains: approximately 15% of global maritime trade volume normally passes through the Red Sea (Kamali et al., 2024). In 2022, 21,344 ships (averaging 59 a day) traversed the route. As attacks mounted, shippers rerouted their vessels via the Cape of Good Hope, a diversion that added between 3,000 and 6,000 nautical miles and two weeks to each trip. Soon, observers estimated that freight container volume crossing the Red Sea fell by 78% compared with the previous year (Duggal & Haddad, 2024), contributing to shipping and production delays and driving up costs for various companies, from carmakers to clothing retailers. The decline in ship traffic through the Suez Canal particularly affects Egypt's economy: canal tolls, estimated at \$9.4

The Houthi campaign directly affected global supply chains. Observers estimated that freight container volume crossing the Red Sea fell by 78% compared with 2023.

billion a year ago, are one of the three most important sources of foreign revenue for the government (Reuters, 2023).

Though Houthi attacks in the Red Sea decreased over time, the security situation remained too volatile to convince shipping companies to redirect their vessels to the area. Moreover, the latest war started by the US and Israel against Iran in February 2026 created a new maritime crisis in the Strait of Hormuz. Following the US-Israeli operation, Iran attacked ports in Gulf countries and threatened to target tankers crossing the Strait. Iranian assertiveness at sea forced Arab states to suspend energy supplies, causing a major disruption to global energy markets. As Iran selectively let some ships cross (largely from Asian countries like China, India, and Malaysia), it executed a de facto toll booth system, coercing companies to pay a fee to avoid attack from Iran (Meade, Raanan, & Diakun, 2026). As of this writing, the US has launched a blockade of Iranian ports in order to force the regime in Tehran to stop its attacks on the Strait of Hormuz.

The Hormuz crisis has put European countries in a delicate position. In several statements, their leaders condemned Iran's action and emphasised freedom of navigation as a fundamental principle of international law (von der Leyen, 2026; Council of the EU, 2026). But though governments across Europe express their desire to ensure safe passage, they refrained from deploying ships. That decision to exercise restraint was largely shaped by Europe's reluctance to join the US-led operation against Iran, whose political objectives they opposed. As a result, European policy discussions circled around the desire to find diplomatic space for a maritime intervention to stabilise the Strait of Hormuz without getting caught in the crossfire between the US, Israel, and Iran. But even if such a space was

found, one inconvenient element of that equation is the fact that European navies may struggle to assemble a sufficiently robust fleet to operate in the Strait. This points to an issue that overshadows our overall security assessment of the southern flank: the lack of credible means for European forces to address the threats and challenges discussed here.

## The erosion of European maritime resources

Despite the many challenges on its southern flank, Europe has yet to respond with increased resources. Numerous statements and policy documents have been released by the EU, or at the national level by its member states, acknowledging the issues and claiming a revived European maritime ambition: for instance, the EU Strategic Compass for Security and Defence in 2022, the revised EU Maritime Security Strategy in 2023, or the EU Action Plan on Cable Security in 2025 highlight the need to address those challenges. But this has not translated into consequential investments regarding the most obvious instrument of such policies, namely, European navies.

The state of European navies remains in 2026 an enduring legacy of the post-Cold War environment. Previous research found that, from 1999 to 2018, European navies lost about 30 percent of their available frigates and destroyers and 20% of their available submarines (Major & Mölling, 2020). Looking more closely, between 2008 and 2012 alone, the number of carriers in European fleets operating in the Mediterranean (including the UK) declined from 5 to 4, frigates and destroyers from 97 to 81, and submarines from 45 to 43, while coastguard vessels increased from 326 to 459 - a shift from warfighting to constabulary ca-

pability at precisely the moment when the security environment was beginning to demand both simultaneously (Codner, 2013: 34). Those sharp cuts in European naval capacities led analysts to warn against Europe's "sea blindness", a concept used to castigate governments' neglect of their naval forces (Stöhs, 2018; Cropsey, 2017).

From that perspective, only a few European countries remain credible naval actors in the Mediterranean. Arguably, the first is France. The French Navy operates 15 principal surface combatants, including FREMM-class frigates; 10 submarines, including 4 nuclear SSBNs and 6 Barracuda nuclear attack submarines; and one aircraft carrier, the Charles de Gaulle, which was most recently deployed to the region as a result of the Iran War of 2026. By all indicators, France remains the unrivalled European Mediterranean country capable of projecting power at sea in a rapid fashion.

Second to France is Italy, whose navy, though smaller, remains a major contributor in numerous maritime EU initiatives, such as Operation Sophia, Operation Irini, and Operation Aspides (Parente, 2025). Between 2009 and 2024, Italian annual contributions to Operation Atalanta ranged from €8.7 million to €27 million, with force commitments growing from one frigate and 432 personnel in 2009 to two frigates, four aircraft, and 388 personnel in 2022 (Parente, 2025: 541). For Operation Sophia, Italy's peak 2015 contribution included an aircraft carrier, a submarine, and three aircraft, deploying 1,026 personnel; its training of over 330 Libyan naval personnel contributed to the rescue of 15,000 migrants in 2016, 20,000 in 2017, and 12,000 between January and August 2018. For Operation Irini (2020-2024), Italy maintained both strategic and force command simulta-

neously, spending between €21.3 million and €40.3 million annually (Parente, 2025: 547).

Two other European Navies, Greece and Spain, are worth mentioning, though they face distinct constraints that undermine their ability to play a role on par with France and Italy. Greece has historically maintained high levels of defence expenditures, particularly in the naval domain. Its armed forces rely on 9 active conventional submarines and 13 principal surface combatants, making them one of the largest fleets in the Mediterranean (IISS, 2026: 103). However, Greek naval posture is heavily influenced by its rivalry with Türkiye, and as a result, most of its capabilities have been dedicated to deterring Ankara. This has often limited the ability of European initiatives to rely on Greek contributions.

Meanwhile, Spain's Mediterranean engagement has been more limited than the format of its navy would suggest. With 11 principal surface combatants, including Aegis-capable F-100 frigates, and a defence budget of approximately €25.6 billion in 2025, Spain has the means to play a significant role in many of the crises facing the area (IISS, 2026: 140-141). However, governments in Madrid have maintained a cautious position regarding the country's Mediterranean policy (Stöhs, 2024: 447).

Despite the shortcomings of European navies, they have been regularly deployed on their southern flank to address security challenges, most often through EU or NATO frameworks. As mentioned before, the EU launched Operation Atalanta in 2008, its first-ever naval operation, to counter piracy off the Horn of Africa. The operation has been praised for successfully escorting vessels of the World Food Programme (WFP) across the Gulf

Operation Atalanta has been praised for successfully escorting vessels of the World Food Programme across the Gulf of Aden, and it is estimated that between 2008 and 2022, Atalanta enabled the WFP to deliver more than 10.5 million tons of food supply to the littoral countries in the Horn of Africa.

of Aden. It is estimated that between 2008 and 2022, Atalanta enabled the WFP to deliver more than 10.5 million tons of food supply to the littoral countries in the Horn of Africa (EU Naval Force Operation Atalanta, 2022). More recently, the EU started Operation Irini, whose objective is “to counter illegal arms trafficking, supporting the implementation of the arms embargo on Libya based on the relevant UN Security Council Resolutions” (European Union External Action, 2023).

Likewise, European navies contributed to NATO operation Sea Guardian, launched in 2016 (replacing operation Active Endeavor). Sea Guardian is intended to support maritime situational awareness and maritime counterterrorism. It relies on ships and maritime patrol aircraft dispatched by Canada, Portugal, Spain, the UK, and Türkiye.

Additionally, some European navies were involved in the ad hoc maritime awareness mission in the Strait of Hormuz (EMASOH), also known as Operation Agenor. Launched in November 2019, EMASOH aimed to ensure freedom of navigation by protecting merchant ships against potential attacks in the Persian Gulf. Its headquarters were located at the French Naval Base in the UAE. Created amid tensions between the first Trump presidency and the Iranian regime, EMASOH reflected European governments’ desire to distance themselves from Washington’s “maximum pressure” approach toward Tehran (Samaan, 2020a). Though the diplomatic philosophy behind EMASOH could inspire a European initiative in the current crisis over the reopening of the Strait of Hormuz, the small size of that past initiative in terms of ships and troops is a reminder of the shortcomings Europeans would face in a new, more ambitious mission.

Table 1. Active naval powers in the Mediterranean in 2026 (selection)

| COUNTRY                                                                                                                                   | PRINCIPAL SURFACE COMBATANTS<br>PSC                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                              | SUBMARINES<br>SSBN SSN SSK | PATROL & COASTAL<br>PCC | ACTIVE NAVAL<br>PERSONNEL |
|-------------------------------------------------------------------------------------------------------------------------------------------|----------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|----------------------------|-------------------------|---------------------------|
|  France<br>+ 1 AIRCRAFT CARRIER<br>(CHARLES DE GAULLE) |                                                                                                                                                                                                                                              |                            |                         |                           |

## Avenues of cooperation at sea

The most obvious way to address European shortcomings in their naval policies is to call for an increase in public expenditures on their navies. There are already signs that European governments are committed to significantly reinvesting in their armed forces, including their navies. The most spectacular rise has been Germany, which is expected to spend about €152 billion by 2029, making it by far the largest military on the continent (Werkhauser, 2026). However, Berlin's trajectory also reveals that the ongoing surge in European military expenditures has less to do with challenges on the southern flank than with those on the eastern flank. Procurement priorities are unlikely to focus on modernising and expanding European fleets, but rather on strengthening ground forces and increasing the firepower needed for a high-intensity conflict with Russia. If European commitments to raising their defence budgets will benefit their navies, one should not expect a major change in their order of battle either.

This leads to the realisation that rather than an increase in national programmes, one should instead call for greater cooperation among Europeans and with their regional partners. Such cooperation can take several forms. It can be institutionalised at the level of organisations such as the EU and NATO, which both maintain credible policies in the area, especially regarding maritime security. The EU's ability to coordinate among myriad stakeholders in the maritime space may be its strongest asset. This has led European decision-makers to argue that the EU's centrality in this multi-agency process is its greatest value. As a result, documents such as the *EU Maritime Security Strategy* assert that "the EU will lead in maritime

domain awareness by enhancing information collection and exchange among different maritime sectors" (European Commission, 2023).

The EU concept of "coordinated maritime presences", launched in 2022, captures this cooperative logic. It is conceived as a lightweight and adaptable tool enabling EU member states operating in selected maritime regions to pool information, share assessments, and improve situational awareness (European External Action Service, 2021). A dedicated coordination cell within the EU Military Staff is responsible for identifying specific maritime areas of interest and aligning the activities of the EU, its member states, and local partners in those zones. This approach envisages an EU naval footprint that does not rely on permanently stationed forces in partner states' ports and bases (Fiott, 2022).

After an initial trial in the Gulf of Guinea, a second coordinated maritime presence was established in the North Western Indian Ocean. It spans a broad region from the Strait of Hormuz to the Southern Tropic and from the northern Red Sea to the central Indian Ocean (Council of the European Union, 2022). This mechanism builds on the earlier EU maritime initiative Critical Maritime Routes Indian Ocean (CRIMARIO), launched in 2015, which already includes cooperation with several Middle Eastern states such as Jordan and Saudi Arabia.

One potential way to solidify European partnerships on the southern flank is through cooperation with Gulf states (understood as the six member states of the Gulf Cooperation Council (GCC), i.e., Saudi Arabia, the UAE, Qatar, Oman, Bahrain, and Kuwait). Gulf states have been directly affected by several crises in the Red Sea and the Strait of Hormuz and have dedicated greater resources to

The EU concept of "coordinated maritime presences", launched in 2022, captures this cooperative logic. It is conceived as a lightweight and adaptable tool enabling EU member states operating in selected maritime regions to pool information, share assessments, and improve situational awareness.

modernising their navies in the past decade. Moreover, the EU signalled its desire to deepen its engagement with the Gulf after releasing a “joint communication to the European Parliament and the Council on a strategic partnership with the Gulf” in 2022. The document stated that EU-Gulf cooperation on maritime security “could include de-confliction channels, sharing maritime information, incident prevention and codes of conduct” (European Commission, 2022: 9). A year later, the EU created the position of special representative for the Gulf region, which has been held since then by Italy’s former foreign minister Luigi di Maio (see Chapter 2 for greater details).

In parallel to the EU, NATO also retains a significant role in maritime security in the region. In some cases, it can be argued that NATO, rather than the EU, is the relevant organisation. First, NATO includes Türkiye and the UK, two of the most consequential actors in the Mediterranean. Second, NATO’s military structures remain, to this day, more advanced and more battle-tested than those of the EU. At the same time, NATO’s Mediterranean posture may be affected by the current tensions between the US and Europe. As the transatlantic organisation is closely associated with US foreign policy in the eyes of many Mediterranean partners, European countries have often been reluctant to use it as a vehicle for missions that could be perceived as offensive by littoral states. This explains why Europeans opted for an ad hoc operation, EMASOH, in the Strait of Hormuz in 2019, or an EU operation, Aspides, instead of the US-led Prosperity Guardian. From that perspective, NATO might experience difficulties in deepening its engagement in the region.

In addition to the multilateral level, there are smaller, more ad hoc forms of coop-

eration that Europeans can explore. One example is the minilateral rapprochement between Israel, Greece, and Cyprus in the 2010s. Though it was partly driven by common security concerns about Türkiye, it also reflected shared interests regarding gas exploration in the Eastern Mediterranean Sea. Starting in 2014, the three states convened an annual trilateral summit, later complemented by a ministerial meeting, dubbed “3+1”, that included the US. Then they joined the Egyptian initiative, the East Mediterranean Gas Forum (EMGF), established in 2020. Italy, Palestine, and Jordan also rallied the EMGF as founding members. In the following years, France also joined, while the US, the EU, and the World Bank became observers (Klotsman & Reich 2025).

Another minilateral format worth reviving is the 5+5 Dialogue. Created in 1990 as a new instrument for Euro-Mediterranean cooperation, it involved the foreign ministers of five countries from the northern shores of the Mediterranean - Spain, France, Italy, Malta, and Portugal - and five from the southern shores - Algeria, Libya, Morocco, Mauritania, and Tunisia (Albinyana & Ibáñez, 2021). Political interest in the 5+5 Dialogue fluctuated over the years and was sometimes undermined by the creation of similar, competing initiatives (e.g., the Union for the Mediterranean [UfM], founded in 2008). In recent years, it has been affected by tensions between Algeria and Morocco. Still, maritime security remains a key item on the initiative’s agenda. In the past, this allowed its members to convene consultations on interoperability and hold joint naval exercises.

At the military-industrial level, cooperation could also help address issues related to naval resources. One good example is the ongoing development of the European Patrol Corvette (EPC), which signals

Political interest in the 5+5 Dialogue fluctuated over the years and was sometimes undermined by the creation of similar, competing initiatives such as the Union for the Mediterranean (UfM), founded in 2008.

the resolve of four of those countries (Italy, France, Greece, and Spain) to address the capability gap collectively. Initiated in 2019, the EPC project is to deliver new corvettes by 2030. Two other European countries (Denmark and Norway) joined the project in 2021. The warships should provide European navies with greater capacity to monitor the security environment in the Mediterranean and, if needed, intervene. This involves both diplomatic and industrial cooperation (with national companies such as Fincantieri, Naval Group, and Navantia). It is also supported by the European Defence Fund, which provided €154 million to fund the production of a first prototype (Kington, 2022).

## Conclusion

Europe's southern maritime flank presents a strategic environment that differs fundamentally from the more clearly defined threat landscape on its eastern borders. Rather than a single dominant adversary, the region stretching from the Mediterranean to the Persian Gulf is characterised by the coexistence of multiple, overlapping security challenges. State collapse in countries such as Libya and Yemen has created persistent security vacuums that enable illicit trafficking, piracy, and other forms of maritime instability. At the same time, enduring interstate rivalries - most notably between Algeria and Morocco, Greece and Türkiye, and above all Israel and Iran - create chronic crises that can rapidly spill into the maritime domain and disrupt global trade routes. The recent tensions in the Red Sea and the Strait of Hormuz demonstrate how conflicts originating on land can quickly produce strategic shocks at sea, with direct consequences for European economic and security interests.

Yet this first chapter also highlights a troubling mismatch between the scale of these challenges and the resources European countries can mobilise to address them. Over the past three decades, European navies have experienced a steady contraction in their fleets and operational capacity, reflecting the strategic priorities of the post-Cold War era. While a few states - notably France and Italy - retain the ability to project naval power in the Mediterranean, most European countries lack the means to sustain significant maritime operations independently. As a result, Europe faces growing difficulty in assembling credible naval forces capable of protecting freedom of navigation, stabilising maritime chokepoints, or responding rapidly to emerging crises along its southern flank.

In this context, the most realistic pathway for Europe lies not in expecting a dramatic resurgence of national naval capabilities but in strengthening cooperation at multiple levels. Multilateral frameworks such as the EU and NATO remain essential platforms for coordinating maritime security policies, sharing information, and organising joint operations. Initiatives such as the EU's coordinated maritime presences illustrate how relatively modest national contributions can be combined to produce a more coherent operational picture and a persistent European presence at sea. At the same time, deeper engagement with regional partners - from North African states to the Gulf monarchies - can help build mechanisms for maritime situational awareness, incident prevention, and crisis management.

Complementary forms of cooperation, including minilateral diplomatic formats and joint industrial projects, also offer promising avenues to mitigate Europe's capability gaps. By pooling resources and aligning procurement efforts, Euro-

pean states can partially offset the limitations of their individual fleets while reinforcing interoperability among their naval forces.

Ultimately, securing Europe's southern maritime flank will require acknowledging the structural constraints under which European navies operate. The diversity of threats

in the region demands flexible responses that combine naval capabilities, diplomatic engagement, and coordination with local partners. Europe's challenge is therefore not only to deploy ships, but also to organise the political and cooperative frameworks that allow limited maritime resources to be used more effectively in a complex and volatile strategic environment.

## References

ALBINYANA, R., & IBÁÑEZ, M. (2021). *The 5+5 Dialogue after 30 years: Prospects and Challenges for Western Mediterranean Cooperation*. IEMed. Mediterranean Yearbook 2021. [https://www.iemed.org/wp-content/uploads/2021/08/55-Dialogue-30-years-Prospects-Challenges-Western-Mediterranean-Cooperation\\_MedYearbook2021.pdf](https://www.iemed.org/wp-content/uploads/2021/08/55-Dialogue-30-years-Prospects-Challenges-Western-Mediterranean-Cooperation_MedYearbook2021.pdf)

BARBA, R. (2022). *Morocco-Algeria Conflict: Spain's Role and Medium-term Scenarios deadline*. Universidad de Navarra. <https://en.unav.edu/web/global-affairs/conflict-to-marruecos-algeria-papel-de-espana-y-escenarios-a-medio-plazo>

BOFFEY, D. (2026, March 10). The HMS Dragon row: why has it taken so long to get a UK destroyer to Cyprus?. *The Guardian*. <https://www.theguardian.com/world/2026/mar/10/mod-criticised-after-delay-in-sending-hms-dragon-to-cyprus>

CODNER, M. (2013). *The Security of the Mediterranean Sea*. LSE Ideas, A Strategy for Southern Europe. <https://www.lse.ac.uk/ideas/Assets/Documents/reports/LSE-IDEAS-A-Strategy-for-Southern-Europe.pdf>

COUNCIL OF THE EUROPEAN UNION. (2022). *Council Conclusions on the Implementation of the Coordinated Maritime Presences Concept in the North-Western Indian Ocean*. Council of the European Union. <https://www.consilium.europa.eu/en/press/press-releases/2022/02/21/coordinated-maritime-presences-council-extends-implementation-in-the-gulf-of-guinea-for-2-years-and-establishes-a-new-concept-in-the-north-west-indian-ocean/#:~:text=Building%20on%20this%20positive%20example,Tropic%20and%20from%20the%20North>

CROPSEY, S. (2017). *Seablinkness: How Political Neglect is Choking American Seapower and What to Do about It*. Encounter Books.

DENIZEAU, A. (2021). *Mavi Vatan, the Blue Homeland: the Origins, Influences and Limits of an Ambitious Doctrine for Turkey*. Institut Français des Relations Internationales. [https://www.ifri.org/sites/default/files/migrated\\_files/documents/atoms/files/denizeau\\_mavi\\_vatan\\_turkey\\_2021.pdf](https://www.ifri.org/sites/default/files/migrated_files/documents/atoms/files/denizeau_mavi_vatan_turkey_2021.pdf)

DUGGAL, H., & HADDAD, M. (2024, February 22). Mapping the Red Sea Attacks. *Al Jazeera*. <https://interactive.aljazeera.com/aje/2024/mapping-red-sea-shipping-attacks/>

EUROPEAN UNION NAVAL FORCE OPERATION ATALANTA (EUNAVFOR). (2022). *WFP 3 Million Metric Tons of Food Delivered to Somalia*. European Union Naval Force Operation ATALANTA – EUNAVFOR. <https://eunavfor.eu/news/wfp-3-million-metric-tons-food-delivered-somalia>

EUROPEAN COMMISSION. (2023). *Joint Communication to the European Parliament and the Council on the Update of the EU Maritime Security Strategy and its Action Plan*. European Commission. <https://www.europeansources.info/record/joint-communication-on-the-update-of-the-eu-maritime-security-strategy-and-its-action-plan-an-enhanced-eu-maritime-security-strategy-for-evolving-maritime-threats/#:~:text=It%20seeks%20to%20drive%20forward,Commission%20on%2010%20March%202023>.

EUROPEAN UNION EXTERNAL ACTION SERVICE (EEAS). (2021, January 25). *The EU launches its Coordinated Maritime Presences concept in the Gulf of Guinea* [Press Release]. [https://www.eeas.europa.eu/eeas/eu-launches-its-coordinated-maritime-presences-concept-gulf-guinea\\_en](https://www.eeas.europa.eu/eeas/eu-launches-its-coordinated-maritime-presences-concept-gulf-guinea_en)

EUROPEAN UNION EXTERNAL ACTION SERVICE (EEAS). (2023). *Operation EU-Navfor MED IRINI - June Report*. European Union External Action Service (EEAS). [https://www.eeas.europa.eu/eeas/operation-eunavfor-med-irini-june-report-0\\_en#:~:text=The%20tasks%20of%20Operation%20EUNAVFOR,Security%20Council%20Resolutions%20\(core%20task\)](https://www.eeas.europa.eu/eeas/operation-eunavfor-med-irini-june-report-0_en#:~:text=The%20tasks%20of%20Operation%20EUNAVFOR,Security%20Council%20Resolutions%20(core%20task))

FIOTT, D. (2022). European Maritime Strategies for the Middle East: Struggling for Relevance?. *Middle East Institute-National University of Singapore Insights*, (282), 1-18. <https://mei.nus.edu.sg/publication/insight-282-european-maritime-strategies-for-the-middle-east-struggling-for-relevance/>

HENNEBERG, S., & MEDINI, S. (2025). *An Algeria-Morocco "Peace Deal"? Managing U.S. Diplomacy and Expectations*. PolicyWatch 4125, The Washington Institute for Near East Policy. <https://www.washingtoninstitute.org/policy-analysis/algeria-morocco-peace-deal-managing-us-diplomacy-and-expectations>

INTERNATIONAL CRISIS GROUP. (2023). *An Island Divided: Next Steps for Troubled Cyprus*. Europe Report, International Crisis Group. <https://icg-prod.s3.amazonaws.com/s3fs-public/2023-06/268-cyprus-an-island-divided.pdf>

INTERNATIONAL INSTITUTE FOR STRATEGIC STUDIES. (2026). *The Military Balance 2026*. Routledge.

JACOBS, A. (2020). *Gulf Rivalries and Great Power Competition in Libya*. Arab Gulf States Institute. <https://agsi.org/analysis/gulf-rivalries-and-great-power-competition-in-libya/>

JUNEAU, T. (2024). Saudi Arabia's costly war in Yemen: a neoclassical realist theory of overbalancing. *International Relations* (OnlineFirst), 1-25. <https://journals.sagepub.com/doi/epub/10.1177/00471178241231728>

KOUTANTOU, A., & GUMRUKCU, T. (2023, December 8). Turning a page, Greece and Turkey agree to mend ties. *Reuters*. <https://www.reuters.com/world/greece-turkey-seek-restart-relations-with-meetings-athens-2023-12-06/>

KINGTON, T. (2022, September 9). European Patrol Corvette to get fresh money from EU coffers. *Defense News*.  
<https://www.defensenews.com/global/europe/2022/09/09/european-patrol-corvette-to-get-fresh-money-from-eu-coffers/#:~:text=ROME%20—%20Nations%20teaming%20to%20build,to%20build%20the%20first%20prototype.>

MAJOR, C., & MÖLLING, C. (2020). The EU's Military Legacy: Over-Institutionalised, Under- equipped and Strategically Divided. In D. Fiott (Ed.), *The CSDP in 2020: The EU's Legacy and Ambition in Security and Defence* (pp. 38-49). EU Institute for Security Studies. [https://www.iss.europa.eu/sites/default/files/EUISS-Files/CSDP%20in%202020\\_0.pdf](https://www.iss.europa.eu/sites/default/files/EUISS-Files/CSDP%20in%202020_0.pdf)

OTTAWAY, D. (2024). *Yemen's Houthis Upset US Middle East Security Calculations*. Wilson Center. <https://www.wilsoncenter.org/article/yemens-houthis-upset-us-middle-east-security-calculations>

PARENTE, G. (2025). To lead or to participate? Italy and the European Union's maritime security operations, 2008-2024. *Contemporary Italian Politics*, 17(4), 536-554. <https://doi.org/10.1080/23248823.2025.2543650>

SAMAAN, J.-L. (2016). *The East Mediterranean Triangle at Crossroads*. US Army War College. <https://press.armywarcollege.edu/monographs/303/>

SAMAAN, J.-L. (2020). *Coronavirus, Naval Forces, and Maritime Security in the Strait of Hormuz*. Arab Gulf States Institute in Washington. <https://agsiw.org/coronavirus-naval-forces-and-maritime-security-in-the-strait-of-hormuz/>

SAMAAN, J.-L. (2023). *The minilateral moment in the Middle East: An opportunity for US regional policy?*. Atlantic Council, Issue Brief.  
<https://www.atlanticcouncil.org/in-depth-research-reports/issue-brief/the-minilateral-moment-in-the-middle-east-an-opportunity-for-us-regional-policy/>

STÖHS, J. (2018). Into the Abyss? : European Naval Power in the Post-Cold War Era. *Naval War College Review*, 71(3), 13-40. <https://digital-commons.usnwc.edu/nwc-review/vol71/iss3/4/>

STÖHS, J. (2024). *European Naval Power: From Cold War to Hybrid Wars*. Palgrave MacMillan.

VILLELABEITIA, I. (2011, September 8). "Analysis: Turkey's gunboat diplomacy makes waves in region", Reuters. <https://www.reuters.com/article/us-turkey-israel-gamble-idUSTRE7871WZ20110908>

WENDEL, S. (2024, March 3). How Red Sea attacks could rewire Middle East trade and economic cooperation. *Al Monitor*. <https://www.al-monitor.com/pro/memos/how-red-sea-attacks-could-rewire-middle-east-trade-and-economic-cooperation>

WERKHAUSER, N. (2026, January 29). Germany's Bundeswehr goes on military spending spree. *Deutsche Welle*. <https://www.dw.com/en/germanys-bundeswehr-goes-on-military-spending-spree/a-75716109>

# **Saudi Emirati Rivalry at Sea and Its Implications for European Interests**

**Máté Szalai**

Research Fellow at the Conflict Research

Unit of Clingendael, and Associate

Professor, Corvinus University of Budapest

In the first half of 2026, geopolitical tensions in the Gulf region<sup>3</sup> have escalated rapidly, affecting regional and global maritime security. Most importantly, after the American-Israeli attack against Iran starting on 28 February, Tehran responded with a wide counteroffensive, which included effectively taking control of the Strait of Hormuz, severely disrupting navigation. At the same time, the Yemeni Houthi movement has recurrently threatened to disrupt maritime transport in the Red Sea region (Abdullah, 2026).

Besides the war between the United States (US), Iran, and Israel, several other major conflicts have affected the maritime security of the regions surrounding the Arabian Peninsula in recent times. In December 2025, the geopolitical rivalry between Saudi Arabia and the United Arab Emirates (UAE) intensified, affecting several theatres of conflict in the Mediterranean and the broader Red Sea region, especially Yemen, Sudan, Somalia, and Libya. By mid-2026, it seems that the Iran crisis did not ease tensions but even added another layer.

All these developments expose the EU's security and economy to the geopolitical dynamics of the Gulf region and, more specifically, to their spillover into the maritime domains of the Red Sea and the Mediterranean. Although the Middle Eastern countries' share in the European Union (EU)'s overall energy mix is limited,<sup>4</sup> indirect effects of the conflict have raised energy prices and put significant inflationary pressure on the EU (Kardas, 2026). At the same time, in 2022, close to 23% of all EU imports came from Asia through the Red Sea (EC, 2024), while undersea fibre optic cables going through the region transfer 90% of

data traffic between the two continents (Leccese, 2025 - see also chapter 3 of this study by G. Marchionna). These figures illustrate the EU's exposure to maritime security in its surrounding regions.

The chapter aims to unfold the effects of the two main geopolitical conflicts, the Saudi-Emirati competition and the conflict with Iran, on maritime security in the Red Sea and the Mediterranean regions. The paper seeks to answer two questions: how does the rivalry between Saudi Arabia and the UAE play out in the maritime domain, especially in light of the 2026 war between the US, Israel, and Iran, and how do these developments affect European interests?

To solve this puzzle, the analysis begins with a reflection on maritime competition in the Gulf with a focus on Saudi-Emirati dynamics. This section is followed by an overview of the strategies and presence of Saudi Arabia and the UAE in the Red Sea and the Mediterranean through their networks of political and security partnerships, port infrastructure development, investments, and fleet development. The paper concludes with a discussion on how the Iran crisis impacts this competition, and recommendations for the EU on how to navigate the challenges that emerge from this competition.

## **Maritime competition in the Gulf and the escalation of the Saudi-Emirati rivalry**

The Gulf region has been the theatre of various geopolitical competitions with a strong maritime component since at least

<sup>3</sup> Defined here as the members of the Gulf Cooperation Council (GCC), Iran, Iraq, and Yemen.

<sup>4</sup> Most importantly, 7% of the EU's oil imports came from the GCC countries, and 3.7% of natural gas imports were provided by Qatar in 2025. See EC, 2026a & 2026b.

the 1980s. The four major Gulf wars<sup>5</sup> and multiple other crises and conflicts<sup>6</sup> have repeatedly disrupted maritime commerce in the Persian Gulf, including around the Strait of Hormuz, with significant repercussions in the Red Sea, the Bab al-Mandeb, and the eastern coasts of Africa.

Despite their historical reliance on maritime traffic for both exports and imports, GCC states did not prioritise the maritime domain in their security policy (Mazzuco, 2026). This was partly because, traditionally, it was external great powers that took responsibility for maintaining peace at sea, most notably the United Kingdom (UK) (until the 1970s) and the United States (since the 1990s). Most noticeably, Bahrain hosts the 5<sup>th</sup> fleet of the US Navy and a British maritime base as well.

A considerable shift toward more active naval policies occurred only in the second half of the 2010s, which resulted in the prioritisation of the maritime domain and further investments in naval capabilities. This was motivated especially by four reasons (Vidal, 2025; Mazzuco, 2026):

- Increasing concerns<sup>7</sup> about Washington's commitment to the stability and security of the GCC states.
- The changing security landscape characterised by increasing usage of coercive maritime tactics by Iran and its

non-state allies, especially the Houthi movement in Yemen.

- The implementation of diversification and modernisation plans in the Gulf, especially in Saudi Arabia, which included many projects that are directly linked to (and dependent on) maritime security.<sup>8</sup>
- The strengthening role of smaller GCC states like Qatar and the UAE in regional geopolitics, for whom the maritime domain is particularly salient.

The growing importance of the maritime space increased the competition among the GCC states (Miller, 2025), especially between Saudi Arabia and the UAE. At first, the expansion of Saudi and Emirati interests did not result in a collision: in Yemen, for example, the UAE took an active role in the Saudi-led coalition supporting the internationally recognised government. In 2018, they even announced the "Strategy of Resolve" (MOFA, 2018), a 60-month-long plan to deepen bilateral relations.

However, the partnership slowly degraded into a rivalry in the late 2010s and the early 2020s. From an economic standpoint, Saudi Arabia's accelerated diversification strategy put the two countries in competition for foreign direct investment and prominence in strategic sectors. From a geopolitical perspective, the UAE's foreign and security policy strategy became increasingly independent and assertive under Mohamed

GCC states did not prioritise the maritime domain in their security policy. This was partly because, traditionally, it was external great powers that took responsibility for maintaining peace at sea, most notably the United Kingdom and the United States.

<sup>5</sup> Including the Iran-Iraq War (1980-1988), the Iraqi invasion of Kuwait and its liberation (1990-1991), the American-led invasion of Iraq (2003), and the current US-Israelian-Iranian War (2026-).

<sup>6</sup> Including the Qatar crisis (2017-2021), the Saudi-led intervention in Yemen (2015-), and the 12-Day War between Iran, the US, and Israel (2025).

<sup>7</sup> These concerns primarily emerged after the lacking or limited US response after Houthi attacks on the territory of Gulf states since 2015, most notably after the Abqaiq and Khurais attacks in 2019 and another one against Abu Dhabi in 2021.

<sup>8</sup> For example, in Saudi Vision 2030, several large-scale initiatives were connected to the Red Sea, including multiple port facilities, tourist destinations, and flagship projects like Neom. Similarly, the more diversified Emirati economic model centres on becoming indispensable in strategic sectors such as maritime connectivity, trade infrastructure development, and energy and natural resources. See: Ali, 2024; Ardemagni, 2024; Ardemagni, 2025.

bin Zayed's tenure.<sup>9</sup> This can be explained not just by the Emirati leadership's increasing ambition, which clashed with Riyadh's traditional "big brother" position within the GCC, but also by Riyadh's pursuit of policies without equal consultation with the other Gulf monarchies (Ramani, 2026). At the same time, amid increasing instability, Emirati frustration grew toward Saudi decision-making, which was considered notoriously slow and reactive.

Tensions became visible in the late 2010s as a result of shifting Saudi priorities, a deprioritisation of countering Iranian and Islamist influence, and more focus on strengthening regional stability to support the Saudi economy. This consideration led to a "de-escalatory developmentalist" approach (Hellyer, 2026), particularly in the Red Sea region, that supports central state institutions and border security – even if it comes with finding a *modus vivendi* with previously securitised actors. In contrast, Abu Dhabi continued to focus on countering the actors that could jeopardise national security and Emirati interests. Instead of Riyadh, the UAE saw more value in developing its own network of allies that often-challenged state institutions supported by Saudi Arabia. Such an approach was inevitably overly disruptive, ambitious, and risk-prone by the Saudi government (Lons, 2026), for example, in Sudan, where the UAE supports the Rapid Support Forces (RSF) accused of committing genocide (Mas & Roger, 2026; Misha, 2026).

The competition turned into open conflict in late 2025, when the Emirati-supported Southern Transitional Council (STC) in Yemen clashed with Saudi-supported fac-

tions.<sup>10</sup> The crisis ended with a swift Saudi campaign against the STC, which led to its dissolution and the UAE's withdrawal from the country (Lons, 2026). After these developments, the Saudi-Emirati competition became public, affecting several theatres of conflict, especially in the Horn of Africa.

## **Saudi-Emirati competition: strategies, partners, and maritime influence**

The maritime dimension of the Saudi-Emirati competition is most visible in three policy areas: competing networks, inter-regional port and infrastructure projects, and national fleet development. The rivalry plays out mostly in two regions that are directly or indirectly neighbours of the EU: the Red Sea and the Mediterranean. However, dynamics are different in the two maritime spaces. The Red Sea is characterised by both stable (like Saudi Arabia) and unstable littoral states (like Yemen and Somalia), and the presence of multiple external and regional powers (including the UAE and Turkey) (Rynn & Nickels, 2024). This environment makes the Red Sea region especially exposed to Saudi-Emirati competition. In contrast, the Mediterranean is only a secondary arena for competition, which can be explained by the geographic distance, the more stable littoral states, and a clearer power hierarchy that is dominated by the EU, Turkey, Israel, and Egypt. In this context, the two GCC states are secondary actors, though their influence is visible in Libya and Syria and in their relations

The Mediterranean is only a secondary arena for competition, which can be explained by the geographic distance, the more stable littoral states, and a clearer power hierarchy that is dominated by the EU, Turkey, Israel, and Egypt.

<sup>9</sup> Although Mohamed bin Zayed only became the President of the UAE in 2022, he has wielded considerable influence as the Crown Prince of Abu Dhabi since 2004 and became the *de facto* leader of the country in 2014.

<sup>10</sup> The UAE took this decision after a Saudi-American meeting, during which the Saudi Crown Prince asked President Trump to pressure the UAE over its involvement in Sudan (Nereim, 2026).

with Turkey, Israel, and others.<sup>11</sup> Therefore, the following analysis will focus mostly on the Red Sea with shorter reflections on the Mediterranean region.

## Competing political and security partnerships

Since the late 2010s, Saudi Arabia and the UAE have developed networks of support in the Red Sea region, many of which are effectively in conflict with each other. Table 1 provides a summary of these competing political and security partnerships; however, a few disclaimers are important to bear in mind. The table does not include the level of dependency of specific partners on Saudi Arabia and the UAE, although it significantly varies. Even more importantly, these networks do not represent strict, comprehensive, or exclusive alignments: for example, Egypt, Turkey, and India have strong ties with both Saudi Arabia and the UAE. The categorisation relies on political and security partnerships and overlaps in interests, mostly over geopolitical issues in the Red Sea region, and not comprehensive alliances. Moreover, many actors in the Horn region have learned to utilise the competition between the Gulf states (and global powers), maximising political and economic benefits through changing their alignment behaviour (Donelli & Dentice, 2020). This feature of regional politics is unlikely to change, making these relationships temporary.

With these limitations in mind, a few differences are important to point out in these competitive networks. First, there is a key dissimilarity between the nature of actors involved: for Saudi Arabia, primary allies include state actors, while the UAE relies

more on non-state and sub-state actors. Saudi Arabia tends to cooperate with state institutions, even if they are weak (e.g., in Yemen). In contrast, the UAE is more inclined to cooperate with non-state or sub-state actors that are locally strong. Abu Dhabi also extensively cooperates with two expansionist, strong state actors in the region, Ethiopia and Israel, and has substantial economic and political ties with Egypt; however, in Red Sea geopolitics, Cairo is more aligned with Riyadh than Abu Dhabi.

Second, the Emirati web of partnerships works much more like an actual network than the Saudi one. Although Riyadh attempted to create a multilateral framework involving some of the littoral states in the form of the Red Sea Council in 2020, the initiative is yet to turn into sustained, institutionalised, and practical collaboration (Ardemagni, 2024). The UAE has placed great emphasis on establishing connections and supply routes among the actors it supports, from forces aligned with Khalifa Haftar in Libya to the RSF in Sudan and the semi-autonomous territories in Somalia (Fenton-Harvey, 2026; Husham, 2026).

The primary tool for the Emirati government is to offer military and financial assistance, including weapons and training, and investments (Moriguchi & Mashino, 2025). To maintain the connectivity, it uses its ports (see later) and has established several military bases, especially around the Gulf of Aden (Middle East Eye, 2025). This allows the UAE to find alternative resupply routes to its partners even in case of disruption, as happened after its reported withdrawal from Yemen (Mas & Roger, 2026).

Saudi Arabia tends to cooperate with state institutions, even if they are weak, while in contrast, the UAE is more inclined to cooperate with non-state or sub-state actors that are locally strong.

<sup>11</sup> Although most attention in this analysis is devoted to these two regions, it is worth noting two additional maritime arenas where the effects of the competition are evident: the Persian Gulf and the Indian Ocean (Ardemagni, 2018).

Table 1. Competing political and security partnerships of Saudi Arabia and the UAE

| Region                            | Red Sea region                                                      |                                                             | Extra-regional   |                                            |
|-----------------------------------|---------------------------------------------------------------------|-------------------------------------------------------------|------------------|--------------------------------------------|
| Nature of the actor               | State                                                               | Non-state/<br>sub-state                                     | State            | Non-state/<br>sub-state                    |
| Saudi-leaning political alignment | Egypt, Somalia, Eritrea, Djibouti, the IIRGoY (Yemen) <sup>12</sup> | SAF (Sudan), IIRGoY-affiliated militias (Yemen)             | Turkey, Pakistan |                                            |
| UAE-leaning political alignment   | Ethiopia, Israel                                                    | STC (Yemen), RSF (Sudan), Somaliland and Puntland (Somalia) | India            | Forces aligned with Khalifa Haftar (Libya) |

Note. Elaborated by the author, sourced from Lons (2026).

Saudi Arabia’s developmentalist approach that prioritises domestic economic developments draws more attention to the mainland than the maritime realm.

Both Gulf states engage in multisectoral cooperation with most of their partners with the maritime component being present in one way or another in most of them. This is especially true for the UAE, which considers its influence over maritime connectivity as a special asset, while also trying to solidify its security influence in the region. Since 2021, the UAE has conducted multi-lateral and bilateral maritime exercises with Israel and announced the joint development of an unmanned maritime vessel with Tel Aviv (Dent, 2025). Reportedly, it also provided access for Israel in its port in Somaliland (Abdallah, 2025). Concerning Ethiopia, the Emirates have supported Addis Abeba in establishing secure commercial access to the sea and decreasing the landlocked country’s dependence on Djibouti (IFA, 2025), especially through Somaliland. This endeavour has caused some tensions between Ethiopia and some of its neighbours, especially Eritrea and Somalia with a constant possibility of escalation (Lons, 2026).

In comparison, Saudi Arabia’s developmentalist approach that prioritises domestic economic developments (Ardemagni, 2024) draws more attention to the mainland than the maritime realm. However, that does not translate into neglect. In 2022, Riyadh organised the Red Wave joint naval exercise with the participation of Jordan, Egypt, Sudan, Djibouti, and Yemen (SIS, 2022). In the same year, Riyadh signed a mostly economic-focused joint cooperation agreement with Djibouti that covers maritime transport, institutional cooperation, and exchange of technology (SPA, 2022). Following the increased Houthi activities in the Red Sea since 2023, the naval component has strengthened in Egyptian-Saudi ties as well: for example, in 2025, the Saudi Arabian Royal Armed Forces participated in the US-led Bright Star drills in Egypt that aimed to strengthen interoperability, training, and other forms of collaboration among participants (Shahbazov, 2025).

<sup>12</sup> Internationally Recognised Government of Yemen

In the Mediterranean region, Saudi-Emirati competition is less intense. Similar to the Red Sea, the UAE seems to have a more proactive approach to relationship-building than Saudi Arabia, with the initial intent to balance against Turkish influence (Vidal, 2021). In this effort, the UAE deepened ties with Israel, Greece, Cyprus, France, and, to some extent, Egypt.

Beyond these competing networks, it is worth noting that the two Gulf states' security partnerships continue to overlap. The US remains a primary partner for both Saudi Arabia and the UAE: until the Emirati withdrawal of its participation in 2023, both states took an active part in the Combined Maritime Forces (CMF) multilateral collaboration led by the US (Mazucco, 2026).<sup>13</sup> With multiple task forces, CMF areas of activity include both the Persian Gulf and the Red Sea, with a scope ranging from traditional threats to counter-piracy and smuggling. Saudi Arabia used its position as the coordinator of Combined Task Force 152 to enhance collaboration with Pakistan and other countries to combat seaborne narcotics trade.

At the same time, both Gulf states – similar to their neighbours – seek to diversify their ties with regional and global powers. In the maritime realm, India became a key partner for virtually all GCC states with bilateral exercises organised with all six countries (Miller, 2025). China has also conducted naval drills with both Saudi Arabia and the UAE.

## Port and maritime infrastructure

The GCC states, including Saudi Arabia and the UAE, have long competed in port infrastructure development in their own territories. While traditionally Dubai's Jebel Ali port was the frontrunner in terms of importance, its prominence has been challenged by others like the Jeddah and the King Abdullah Ports in Saudi Arabia, the Khalifa Port in Abu Dhabi, or the Al-Duqum and Salalah ports in Oman.

Internationally, the UAE has much more extensive investments in port infrastructure. Through DP World, a logistics giant created in 2006 closely linked to the ruling family of Dubai, the UAE managed to invest in 60 ports and terminals worldwide (DP World, 2026), several of which are located in the Red Sea, like the Jeddah Port in Saudi Arabia,<sup>14</sup> Berbera in Somaliland and Bosaso in Puntland, and Ain Sokhna Port in Egypt (in the Gulf of Suez). In the Mediterranean, Limassol (Cyprus), the Djazair and Djen Djen ports (Algeria), and Marseille (France) are key facilities with DP World investment. Additionally, the Emirati company gained the rights to develop the Tartus port (Syria), further increasing its share in maritime commerce in the Mediterranean.

Although DP World is primarily an economic enterprise, it plays an important political and security role too. It cooperates with the US in counter-terrorism and conducts counter-piracy activities (Kocak, 2020).<sup>15</sup> The economic network of the company can be used to control maritime trade, counter competition, and extend footprint

Beyond Sudan, Somaliland represents the most likely arena of escalation in the region between Saudi Arabia and the UAE.

<sup>13</sup> Although the UAE officially announced the withdrawal of its participation, CMF continues to list the UAE as a partner.

<sup>14</sup> The Jeddah Port has been probably the most strategic investments of DP World. This is why it was notable that, in February 2026, the company sold 37.5% share in the southern container terminal to a Danish company (Mathews, 2026).

<sup>15</sup> DP World was the first international port operator certified as a partner in the US Customs-Trade Partnership Against Terrorism Initiative in 2008. It organises conferences and conducts security and policing activities.

and influence beyond the ports. The company was also accused by Ukraine of supporting Russian sanctions evasion and arms transfers (NACP, 2023).

Another key company in the UAE is the AD Ports Group, which has stakes in 35 terminals worldwide, including Adabiya and Safaga in Egypt, Aqaba in Jordan, Latakia in Syria, and 15 terminals in Spain, showcasing an extended network in the Mediterranean and the Red Sea (AD Ports, 2026). Although DP World has a much larger public profile, the AD Ports Group's investment strategy is more risk-prone: while the former follows existing trade routes that had proven their viability, the latter is willing to take more risks, invests more in technological innovation, and contributes to the emergence of new trade routes (Container News, 2025).

That being said, Abu Dhabi has faced some setbacks since the escalation of tensions with Riyadh. Most importantly, the UAE had to give up its foothold in the southern seashore of Yemen and, more importantly, the island of Socotra, which had been under Emirati influence for a decade (Ardemagni, 2018). In January 2026, the government of Somalia also cancelled all defence agreements with the UAE and ceased official cooperation over several ports, including those in Berbera, Bosaso, and Kismayo. However, in practice, DP World continues to operate the Berbera port, located in the de facto autonomous Somaliland, beyond the reach of the federal government. In February 2026, Abu Dhabi even outlined the "Green Berbera Vision", a solar plant construction project (Dutton, 2026). It is also not clear if the initially reported withdrawal from

Bosaso has been completed, especially given the UAE's role in the security architecture of Putland (Paes, 2026). At the same time, Jubaland also rejected the federal government's cancellation of treaties concerning Kismayo (Malna, 2026).

Beyond Sudan, Somaliland represents the most likely arena of escalation in the region between Saudi Arabia and the UAE (Fenton-Harvey, 2026). The escalation in December in Yemen coincided with the Israeli recognition of Somaliland's independence, becoming the first state to recognise the secessionist territory. This indicated coordinated action by Israel and the UAE. Moreover, after the US-Israeli attacks on Iran, Bloomberg reported that Israel is seeking to establish a military base (Mark, 2026). There are indeed indications of further Emirati-Israeli cooperation in Somaliland and beyond (Cafiero, 2026).

Even after the pushback against Emirati influence,<sup>16</sup> Saudi Arabia lags behind the UAE in maritime investments in both regions (Clynch, 2026). This could be explained by the more inward-looking nature of Saudi economic development and a larger incentive for the UAE to compensate for its small size. Additionally, Saudi Arabia does not have a flagship company that can be compared to the global influence of DP World as a port operator. While the country has significant actors in the sector, such as Bahri or the Saudi Global Ports, these do not match either the profile or the influence of DP World. Similar to other industries, the largest Saudi sovereign wealth fund, the Public Investment Fund (PIF), plays an outstand-

<sup>16</sup> While the scale of the Emirati drawback in early 2026 is without precedent, the UAE has faced difficulties before. In 2018, Djibouti cancelled an agreement with DP World, expelled its staff from the country and replaced the Emirati company with a Chinese one. The incident was followed by legal battles that ultimately favoured Djibouti's case (Mizner, 2025).

ing role as an investor in infrastructure and logistics, primarily through subsidiaries. However, PIF does not operate a comparable international port network.

## National fleet development

In the last decade, the GCC states have significantly upped their naval capabilities. Saudi Arabia initiated the Saudi Naval Expansion Programme II (SNEP II) that aims to significantly upgrade the Saudi naval force (Vidal, 2025). Between 2014 and 2024, Riyadh managed to secure a number of high-calibre purchase deals, mostly from American and European suppliers. This includes 12 frigates from Spanish and American companies and various types of patrol boats. The programme is overseen by two main institutions created in 2017, namely the Saudi Arabia's General Authority for Military Industries (GAMI) and the Saudi Arabian Military Industries (SAMI) (Miller, 2025).

As a result of the programme, the Saudi government significantly upgraded their military forces, especially through the development of the navy's Western Fleet based in Jeddah and the Saudi Border Guards' maritime component (Ardemagni, 2024). With these, Riyadh has improved capabilities that enable the country to strengthen its naval defensive posture, participate in various multilateral missions, and combat hybrid threats from the sea, including smuggling.

However, the Saudi strategy's weakness is a focus on quantity over quality (Vidal, 2024: 8). Modernisation of old vessels, which constitute the majority of the fleet, is not considered a priority. The Saudi maritime capabilities are lagging behind in unmanned technologies, as well as in building up proper training and an "ethos" for naval careers compared to other branches of the military (Vidal, 2024: 8-13).

While there is no official programme, the UAE also upgraded its fleet in the last 10 years with several frigates, corvettes, and patrol crafts (Miller, 2025), becoming one of the most capable maritime powers in the region (Ali, 2025). With a multi-stage procurement strategy, the UAE first built up its defensive capabilities to strengthen deterrence against seaborne attacks, then improved its ability to conduct limited and increasingly wider operations on open seas as well (Mazzuco, 2023).

In contrast with Saudi Arabia, the Emirati strategy has prioritised quality even with lower quantities. Realising its inability to compete with Saudi Arabia in quantitative rivalry, the UAE has put emphasis on local shipbuilding and unmanned technologies much earlier than Saudi Arabia and established a more extensive environment for training with at least 12 commercial academies (Vidal, 2024: 14-21).

Beyond purchases, the two Gulf states increasingly aim to develop their national defence industries in the maritime realm as well (Mazzuco, 2023). In this competition, the UAE is ahead of Saudi Arabia and the rest: the Emirati EDGE Group and its subsidiaries have managed to build up considerable industrial capacities (Miller, 2025).

## Effects of the US-Israeli-Iranian war

The US-Israeli attack on Iran and its consequences had direct consequences on the Saudi-Emirati competition and the maritime security in different regions. Instead of de-escalation, the conflict gave another layer to the Saudi-Emirati competition and reinforced the foundations of the current competing strategies in Riyadh and Abu Dhabi (Filiu, 2026; Ramani, 2026).

Riyadh has improved capabilities that enable the country to strengthen its naval defensive posture, participate in various multilateral missions, and combat hybrid threats from the sea, including smuggling.

Furthermore, strategic thinking in the Gulf is increasingly shaped by balance-of-power calculations (Al-Etaibi, 2026). These considerations will likely put Saudi Arabia and the UAE further at odds with each other. With Iran weakened, the US-backed Israel seems to occupy a more dominant position. While the war only increased the Saudi leadership's mistrust of Israel, the UAE seems to double down on its partnership with the country. In this context, the UAE's setback in Yemen would only lead to a temporary tactical retreat rather than a strategic reassessment of aims and alliances.

The competition is likely to proceed in the maritime realm as well. The disruption at the Strait of Hormuz highlighted the GCC states' inability to secure the most critical naval chokepoint for their economies. Moreover, it is not only the Persian Gulf but also the Red Sea that have gained importance (Calabrese, 2026; EPC, 2026): as GCC states look for alternative routes, the value of the East-West pipeline in Saudi Arabia, which connects Abqaiq with the Yanbu port, has increased. All these will likely incentivise both states to strengthen their own influence, which, coupled with a zero-sum mentality, can further escalate the rivalry.

Additionally, the exposure of the security of the GCC states to the Houthi movement was once again highlighted. During the war, the Yemeni group served as a successful deterrent against the GCC states conducting meaningful offensive action against Iran and kept them in check with constant threats about disrupting maritime travel in the Red Sea. Even after the potential resolution of the conflict with Iran, such an exposure to Yemen will be one of the key geopolitical challenges the GCC states are going to face in the foreseeable future.

## European interests and the Saudi-Emirati rivalry

While the EU and its member states have a proactive strategy and dominant presence in the Mediterranean, the Red Sea remains on the verge of political attention. Even as regional developments have persistently highlighted the EU's exposure, the promised European Middle East strategy is continually postponed.

The cases of the various maritime missions showcase this problem. Operations like EU NAVFOR Atalanta (2008-), Aspides (2024-), or the US-led Operation Prosperity Guardian (2023-2025) remained reactive in nature and only serve to mitigate some of the threats emanating from the region, including those posed by piracy and the Houthi movement. Without a more comprehensive answer to the broader security, political, and economic challenges affecting the region, these military operations remain limited in efficiency and scope.

A more active role would necessitate the formation of an independent Red Sea strategy that encompasses policies on conflicts in Yemen, Somalia, and Sudan, as well as maritime security and infrastructure development. This would also strengthen the EU's credibility as an important partner for the Gulf in the region. A more strategic approach could even mitigate the weakness of the EU and its member states emanating from its relatively limited naval capabilities compared to other stakeholders.

In a European Red Sea strategy, cooperation with the GCC will definitely play an important role – as the US-Israeli-Iranian war shows, there is increased synergy between European and the perspectives of multiple GCC states on

The disruption at the Strait of Hormuz highlighted the GCC states' inability to secure the most critical naval chokepoint for their economies.

avoiding escalation, putting political capital into mediation, keeping the law of the sea intact, and mitigating the economic, environmental, and security spillovers (Al-Suwaidi, 2026; Bueger, 2025). The conflicts in the last year, including the wars in Gaza, Sudan, and Iran, weakened many international legal norms, including those related to the protection of civilians. Adding to this, the Houthis' threats over the Red Sea and the Iranian control over the Strait of Hormuz made the weaponisation of maritime chokepoints a recurring element of warfare. Avoiding similar scenarios in the future, in addition to the protection of maritime infrastructure, including ports and deep-sea internet cables, should be a priority in EU-GCC collaboration and will require proactive steps by both sides.

Beyond the lack of a clear strategy, the Saudi-Emirati competition also puts the EU in a challenging position. Beyond avoiding taking sides, the EU has not responded meaningfully to the conflict. In formulating a response, European decision-makers should consider two important perspectives. First, different theatres require different policy responses and a one-size-fits-all approach will not be successful. Second, however, in recent years, relations with the UAE developed much more rapidly than those with Saudi Arabia. This is evidenced by, for example, the start of free trade negotiations individually with the UAE without similar initiatives with Saudi Arabia and the other GCC states. Coupled with more intensive collaboration at the state level between the UAE and EU member states, the Union risks drifting de facto further towards the UAE or being perceived as siding with it, despite its relatively stronger alignment with Saudi Arabia in terms of specific regional conflicts. This is especially threatening if the post-war balance of power calculations put the two Gulf states in greater conflict with each other.

Although by proclaiming neutrality, the EU successfully avoided negative consequences in the Qatar crisis (2017-2021), the current situation may be different. Since 2021, the EU has aspired to become a more important partner for the GCC, upgrading diplomatic engagement and intensifying political and economic ties. Moreover, the Saudi-Emirati competition affects European interests in the Red Sea more directly. Both states have larger financial and military capabilities than Qatar, making escalation between them more intense. Without addressing these challenges, the EU risks the degradation of its position.

This perspective also highlights that the traditional interregional approach favoured by the EU in building EU-GCC relations is not the most effective way to build ties. In contrast, individual collaboration with GCC states could make more sense in most portfolios. Such an approach could especially be effective in supporting the national defence industries of GCC states and finding opportunities to engage in joint mediation in the region. All these could lead to more organic and active collaboration with the GCC states and an enlarged influence in maritime security developments in neighbouring regions of the EU.

## Conclusion and recommendations

The analysis showed that maintaining maritime security in the neighbouring regions of the EU became more complicated than before. Regardless of the US-Israeli-Iranian war, Saudi Arabia and the UAE will remain important regional maritime players and continue to compete with each other. The outcome of this rivalry cannot be determined at this point, as both states have considerable competitive

There is increased synergy between European and the perspectives of multiple GCC states on avoiding escalation, putting political capital into mediation, keeping the law of the sea intact, and mitigating the economic, environmental, and security spillover.

Since 2021, the EU has aspired to become a more important partner for the GCC, upgrading diplomatic engagement and intensifying political and economic ties.

advantages. On the one hand, Saudi Arabia has a larger size and capabilities (including naval capabilities), geopolitical depth, and direct access to both the Red Sea and the Gulf. However, slow decision-making and the lack of a coherent strategy in influence-building somewhat undermine the Saudi position. In contrast, despite its smaller size, the UAE has a more proactive and assertive strategy, a more quality-focused naval development trajectory, and it benefits from being the first mover in many domains (including maritime infrastructure investments in the region).

The fact that the UAE is willing to take more risks is both an advantage and a disadvantage. On the one hand, it allows the Emirati leadership to make bold choices and shape local developments before Riyadh can react. On the other, however, this attitude leads to strategic mistakes (including the escalation in Yemen that resulted in Emirati withdrawal) and high chances of antagonising local actors (like Somalia or Egypt). The neglect of normative considerations has already led the UAE to cooperate with highly contentious actors like the RSF in Sudan, which not only results in a political backlash against the country but also deepens humanitarian crises and further undermines international law.

Amidst this rivalry and the anticipated increase in maritime politics in neighbouring regions, there are several steps that can be taken by the EU to increase its influence and maritime security in the Red Sea and beyond:

- formulate a comprehensive Red Sea strategy that encompasses policies towards the main theatres of conflict, as well as the maritime realm;
- engage in more sustained, proactive, and comprehensive maritime security initiatives instead of reactive and limited defensive coalitions;
- support maritime connectivity projects that can be supported by both sides;
- increase the role of maritime cooperation with both the GCC and its members, prioritising the defence of the law of the sea and the protection of maritime chokepoints;
- maintain neutrality in the Saudi-Emirati competition while deepening collaboration with both sides in areas of mutual interest and balance bilateral ties with Saudi Arabia and the UAE more strategically
- use regulations to incentivise defence industry collaboration between EU and GCC states while advancing proper safeguards, and to intensify spillovers to other sectors.

## References

ABDALLAH, S. (2025, December 12). The Red Sea Shifts from Saudi Control to Global Power Rivalry. *Al-Hurra*. <https://alhurra.com/en/9731>.

AD Ports (2026). *AD Ports at a Glance* [Infographic]. AD Ports Group. <https://www.adportsgroup.com/en/investors/infographic>

ALI, L. (2025). *Maritime Security and Trade Corridors – Connecting the Red Sea to the Indo-Pacific and the Relevance to the Gulf*. Gulf Research Center. <https://www.grc.net/single-commentary/335>.

AL-ETAIBI, A.B. (2026). *How the Gulf States Can Navigate the Middle East's New Alliance Politics*. Middle East Council on Global Affairs. [https://mecouncil.org/blog\\_posts/how-the-gulf-states-can-navigate-the-middle-east-s-new-alliance-politics/](https://mecouncil.org/blog_posts/how-the-gulf-states-can-navigate-the-middle-east-s-new-alliance-politics/).

AL-SUWAIDI, K. (2026). *A Critical Evaluation of the GCC-EU Strategic Partnership*. Anwar Gargash Diplomatic Academy. <https://www.agda.ac.ae/research/publications-multimedia-events/publication-details/a-critical-evaluation-of-the-gcc-eu-strategic-partnership>.

ARAB NEWS. (2022, June 4). Saudi Arabia's Red Wave 5 Joint Naval Drill Wraps Up. *Arab News*. <https://www.arabnews.com/node/2096311/saudi-arabia>.

ARDEMAGNI, E. (2018). *Gulf Powers: Maritime Rivalry in the Western Indian Ocean*. ISPI. <https://www.ispionline.it/en/publication/gulf-powers-maritime-rivalry-western-indian-ocean-20212>.

ARDEMAGNI, E. (2024). *Saudi Arabia Has a Red Sea Vision, not yet a Strategy*. Arab Gulf States Institute. <https://agsi.org/analysis/saudi-arabia-has-a-red-sea-vision-not-yet-a-strategy/>.

ARDEMAGNI, E. (2025). *The GCC States' Security Policies in the Red Sea Geopolitical Border: Factors and Policy Options*. LUISS. <https://mp.luiss.it/wp-content/uploads/2025/06/ArdemagniPAPER.pdf>.

BUEGER, C. (2025). *Seas of Convergence: EU-GCC Maritime Security Cooperation in the Western Indian Ocean*. Trends Institute. <https://trendsresearch.org/insight/seas-of-convergence-eu-gcc-maritime-security-cooperation-in-the-western-indian-ocean/>.

CALABRESE, J. (2026). *Saudi Arabia's Somalia Gambit*. Gulf International Forum. <https://gulfif.org/saudi-arabias-somalia-gambit/>.

CLYNCH, H. (2026, March 3). UAE and Saudi Arabia Vie for African Influence. *African Business*. <https://african.business/2026/03/trade-investment/uae-and-saudi-arabia-vie-for-african-influence>.

COUNCIL OF THE EUROPEAN UNION. (2026a). *Where does the EU get its oil from?*. Council of the European Union. <https://www.consilium.europa.eu/en/info-graphics/where-does-the-eu-get-its-oil-from/>.

COUNCIL OF THE EUROPEAN UNION. (2026b). *Where does the EU's gas come from*. Council of the European Union. <https://www.consilium.europa.eu/en/info-graphics/where-does-the-eu-s-gas-come-from/>.

DENT, E. (2025). *Israel-UAE Defense Cooperation Grows under the Abraham Accords*. PolicyWatch 4087, The Washington Institute for Near East Policy. <https://www.washingtoninstitute.org/policy-analysis/israel-uae-defense-cooperation-grows-under-abraham-accords>.

DONELLI, F., & DENTICE, G. (2020). Fluctuating Saudi and Emirati Alignment Behaviours in the Horn of Africa. *The International Spectator*, 55(1), 126–142. [https://arts.units.it/retrieve/dc9ddf89-50b8-41b2-acfe-a0cf9c43d157/Girometti+2022-Post\\_print.pdf](https://arts.units.it/retrieve/dc9ddf89-50b8-41b2-acfe-a0cf9c43d157/Girometti+2022-Post_print.pdf)

DP WORLD. (2026). *Our Locations*. <https://www.dpworld.com/en/about-us/our-locations>.

DUTTON, J. (2026, February 18). Unfazed by Saudi Pressure, UAE Unveils Solar Investment in Somaliland. *Al-Monitor*. <https://www.al-monitor.com/originals/2026/02/unfazed-saudi-pressure-uae-unveils-solar-investment-somaliland>.

EUROPEAN COMMISSION. (2024). *Impact of the Red Sea Crisis on Economic Outlook*. European Commission. [https://ec.europa.eu/economy\\_finance/forecasts/2024/winter/01%20-%20Red%20Sea.pdf](https://ec.europa.eu/economy_finance/forecasts/2024/winter/01%20-%20Red%20Sea.pdf).

EMIRATES POLICY CENTRE (EPC). (2026). *Exacerbating the Risk of Fragility: Consequences of Iran War on the Red Sea and the Horn of Africa Region*. Emirates Policy Centre (EPC). <https://epc.ae/en/details/brief/exacerbating-the-risk-of-fragility-consequences-of-iran-war-on-the-red-sea-and-the-horn-of-africa-region>

FENTON-HARVEY, J. (2026, February 9). The Growing Saudi-UAE Power Struggle in the Horn of Africa. *The New Arab*. <https://www.newarab.com/analysis/growing-saudi-uae-power-struggle-horn-africa>.

FILIU, J. (2026, April 5). The Power Struggle between Saudi Arabia and the UAE is only on Hold. *Le Monde*. [https://www.lemonde.fr/en/opinion/article/2026/04/05/the-power-struggle-between-saudi-arabia-and-the-uae-is-only-on-hold\\_6752140\\_23.html](https://www.lemonde.fr/en/opinion/article/2026/04/05/the-power-struggle-between-saudi-arabia-and-the-uae-is-only-on-hold_6752140_23.html).

HELLYER, H.A. (2026). *Risk, Order, and Power: The Saudi-Emirati Divergence*. War on the Rocks. <https://warontherocks.com/2026/01/risk-order-and-power-the-saudi-emirati-divergence/>.

HUSHAM, E. (2026, March 27). The UAE's Quiet Empire. *New Internationalist*. <https://newint.org/military/2026/uaes-quiet-empire>.

ITIMOUDIS, A. (2025, February 19). Analysis: Behind DP World and AD Ports Group Investment Strategy. *Container News*. <https://container-news.com/analysis-behind-dp-world-and-ad-ports-group-investment-strategy/>

KARDAS, S. (2026). *Gimme Fuel, Hold the Fire: How Europe Can Safeguard its Energy Security against Gulf Shocks*. European Council on Foreign Relations. <https://ecfr.eu/article/gimme-fuel-hold-the-fire-how-europe-can-safeguard-its-energy-security-against-gulf-shocks/>.

KOCAK, A. (2020). *Dubai Ports World as the UAE Foreign Policy Tool*. Clingendael Institute. <https://www.clingendael.org/publication/dubai-ports-world-uae-foreign-policy-tool>.

LECCESE, G. (2025). *Chokepoint Above and Below the Surface: The Red Sea's Emerging Infrastructure Challenge*. Istituto Affari Internazionali (IAI). <https://www.iai.it/en/publications/c41/chokepoint-above-and-below-surface-red-seas-emerging-infrastructure-challenge>.

LONS, C. (2026). *Power Struggle: What the Saudi-UAE Rivalry Means for the Red Sea – and Europe*. European Council on Foreign Relations. <https://ecfr.eu/article/power-struggle-what-the-saudi-uae-rivalry-means-for-the-red-sea-and-europe/>.

MALNA, C. (2026, January 26). Somalia-UAE Port Dispute Deepens, Carrying Implications for Kenya. *The Kenyan Wall Street*. <https://kenyanwallstreet.com/somalia-uae-port-dispute-deepens-carrying-implications-for-kenya>.

MARK, S. (2026, March 11). Israel Plans New Foothold on the Red Sea to Fight the Houthis. *Bloomberg*. <https://www.bloomberg.com/news/features/2026-03-11/israel-eyes-red-sea-base-in-somaliland-to-fight-iran-backed-houthis>.

MAS, L., & ROGER, B. (2026, March 22). The UAE Reorganises Its Arms Supply Network for Sudanese Paramilitaries. *Le Monde*. [https://www.lemonde.fr/en/le-monde-africa/article/2026/03/22/the-uae-is-reorganizing-its-arms-supply-network-for-sudanese-paramilitaries\\_6751682\\_124.html](https://www.lemonde.fr/en/le-monde-africa/article/2026/03/22/the-uae-is-reorganizing-its-arms-supply-network-for-sudanese-paramilitaries_6751682_124.html).

MATHEWS, S. (2026, February 19). DP World Sells Partial Stake in Saudi Arabia's Jeddah Islamic Port. *Middle East Eye*. <https://www.middleeasteye.net/news/dp-world-sales-partial-stake-saudi-arabias-jeddah-islamic-port>.

MAZZUCO, L.J.M. (2023). *Targeted Acquisitions, Major Commissions: The UAE's Dual Track Approach to the Naval Defense Sector*. Arab Gulf States In-

stitute. <https://agsi.org/analysis/targeted-acquisitions-major-commissions-the-uaes-dual-approach-to-the-naval-defense-sector/>.

MAZZUCO, L. J. M. (2026). *Gulf Maritime Security: Balancing Partnerships and Flexibility*. Arab Gulf States Institute. <https://agsi.org/analysis/gulf-maritime-security-balancing-partnership-and-flexibility/>.

RICKETT, O. (2025, October 2). How the UAE Built a Circle of Bases to Control the Gulf of Aden. *Middle East Eye*. <https://www.middleeasteye.net/news/uae-yemen-somalia-circle-bases-control-gulf-of-aden>.

MILLER, R. (2025). *Navigating Rocky Waters: GCC Strategies for Maritime Security*. Middle East Council on Global Affairs. <https://mecouncil.org/publication/navigating-rocky-waters-gcc-strategies-for-maritime-security/>.

MISHA, V. (2026, February 16). Sudan: 'Hallmark of Genocide' Found in El Fasher UN Investigators Detail Mass Killing and Ethnic Targeting. *United Nations News*. <https://news.un.org/en/story/2026/02/1166997>.

MIZNER, A. (2025, October 8). DP World Setback in Djibouti Port Saga. *African Law & Business*. <https://www.africanlawbusiness.com/news/dp-world-setback-in-djibouti-port-saga/>.

MORIGUCHI, J., & MASHINO, I. (2025). *The UAE's Strategy in Africa – Aiming to Strengthen Logistics Networks by Acquiring Key Port Concessions*. Mitsui & Co. [https://www.mitsui.com/mgssi/en/report/detail/\\_\\_\\_icsFiles/afieldfile/2025/03/09/2501\\_e\\_mashino\\_e.pdf](https://www.mitsui.com/mgssi/en/report/detail/___icsFiles/afieldfile/2025/03/09/2501_e_mashino_e.pdf).

NATIONAL AGENCY ON CORRUPTION PREVENTION (NACP). (2023). *DP World, One of the World's Largest Port Operators, Added to the List of International War Sponsors*. NACP. <https://nazk.gov.ua/en/dp-world-one-of-the-world-s-largest-port-operators-added-to-the-list-of-international-war-sponsors/>.

PAES, W.-C., BEALES, E., VIDAL RIBE, A., & FACCENDA M. (2026). *Lawless Seas, Contested Shores – Piracy, Smuggling, and the Scramble for Port Access in the Horn of Africa*. International Institute for Strategic Studies. <https://www.iiss.org/research-paper/2026/01/lawless-seas-contested-shores—piracy-smuggling-and-the-scramble-for-port-access-in-the-horn-of-africa/>.

RAMANI, S. (2026). *The Saudi-UAE Rift, a High Stakes Strategic Rivalry*. CRI. <https://www.cri.ltd/news-insights/the-saudi-uae-rift-a-high-stakes-strategic-rivalry>.

RYNN, S., & NICKELS, B. (2024). *Enhancing Security in the Red Sea Arena*. George C. Marshall European Center for Security Studies. <https://www.marshall-center.org/en/publications/clock-tower-security-series/enhancing-security-red-sea-arena/enhancing-security-red-sea-arena>.

SEID, M. (2025). *Forging Ahead: Charting the Next Phase in Ethiopia-UAE Strategic Partnership*. Institute of Foreign Affairs, Federal Democratic Republic of Ethiopia. <https://www.ifa.gov.et/2025/04/15/forging-ahead-charting-the-next-phase-in-the-ethiopia-uae-strategic-partnership/>.

SHAHBAZOV, F. (2025). *Egypt and Saudi Arabia Construct a New Strategic Naval Axis*. Stimson Institute. <https://www.stimson.org/2025/egypt-and-saudi-arabia-construct-a-new-strategic-naval-axis/>.

SAUDI PRESS AGENCY (SPA). (2022). *Saudi Arabia, Djibouti Sign Joint Cooperation Agreement on Maritime Transport*. SAUDI Press Agency, Kingdom of Saudi Arabia. <https://www.spa.gov.sa/2365027>.

UNITED ARAB EMIRATES MINISTRY OF FOREIGN AFFAIRS. (2018). *UAE, Saudi Arabia Announce Joint Vision, Strategic Partnership across 44 Economic, Developmental, Military Projects*. United Arab Emirates Ministry of Foreign Affairs. <https://www.mofa.gov.ae/en/mediahub/news/2019/2018/6/7/07-06-2018-uae-saudi-arabia>.

VIDAL, A. (2021). *The United Arab Emirates: A Mediterranean Power?*. Instituto Español de Estudios Estratégicos. [https://www.ieee.es/Galerias/fichero/docs\\_opinion/2021/DIEEEO81\\_2021\\_ALBVID\\_Emiratos\\_ENG.pdf](https://www.ieee.es/Galerias/fichero/docs_opinion/2021/DIEEEO81_2021_ALBVID_Emiratos_ENG.pdf).

VIDAL, A. (2024). *Securing the Seas. Examining Changing Saudi & Emirati Naval Capabilities*. Gulf International Forum. <https://gulfif.org/app/wp-content/uploads/2024/04/Securing-the-Seas-Saudi-Emirati-Different-Naval-Capabilities-and-Strategies-.pdf>.

VIDAL, A. (2025). *Shopping for Sea Power: Saudi Arabia's Naval Transformation*. Institute for International Strategic Studies. <https://www.iiss.org/online-analysis/military-balance/2025/10/shopping-for-sea-power-saudi-arabias-naval-transformation/>.



# **Keeping the Mediterranean Connected: How Cable Disruptions Can Escalate Maritime Crises**

**Gianmarco Gabriele Marchionna**  
Research Fellow LUISS University - Center  
for International and Strategic Studies  
(CISS)

## Introduction

Submarine cables now constitute a critical layer of the Mediterranean security environment, supporting the data flows on which economic activity, government communications, and maritime operations increasingly depend. Yet disruptions affecting these systems are still often treated as technical incidents rather than as potential drivers of wider political and military crises.

This chapter examines the conditions under which a cable disruption in the Mediterranean can escalate into a broader security crisis. Its core argument is that the main risk lies not only in physical vulnerability, but in the interaction between infrastructure concentration, attribution ambiguity, geopolitical tension, and fragmented governance. In a region marked by contested maritime spaces and growing dependence on digital connectivity, even a limited disruption can generate effects that extend well beyond the infrastructure itself. From a European perspective, this exposure is structural rather than episodic, reflecting route concentration, limited industrial depth, and dependence on foreign-controlled cable infrastructure.

The chapter has two aims. First, it maps the main threat categories affecting Mediterranean cable infrastructure. Second, it analyses how technical disruption can acquire political and military significance through three empirical cases. The final section identifies the main governance gaps and translates them into practical recommendations.

### **A fragile backbone: the digital risk landscape of the Mediterranean**

The Mediterranean is home to a critical digital infrastructure, a dense web of sub-

marine cables, landing stations, and port digitalisation systems whose disruption carries consequences far beyond the domains traditionally monitored by maritime security analysts (Wall & Morcos, 2021). As the basin consolidates its role as a geopolitical crossroads connecting the Indo-Pacific to Europe, this infrastructure remains under-governed and under-analysed. This section maps the risk landscape across the Eastern, Aegean, and Central Mediterranean - examining the physical, cyber, and hybrid threats affecting them, alongside the cascading pressures generated by the ongoing crises in the Red Sea and the Strait of Hormuz, which by March 2026 had produced an unprecedented simultaneous disruption of both major maritime data chokepoints linking Europe to Asia and Africa (Moody, Tzourbakis, & Abdullahi, 2024).

### **The physical layer: routes, nodes, and chokepoints**

Around 17 cable systems crossing the Red Sea carry much of the data traffic between Europe, Asia, and Africa, passing through Egyptian territorial waters before landing at hub stations in Marseille, Palermo, Genoa, Trieste, and Alexandria -

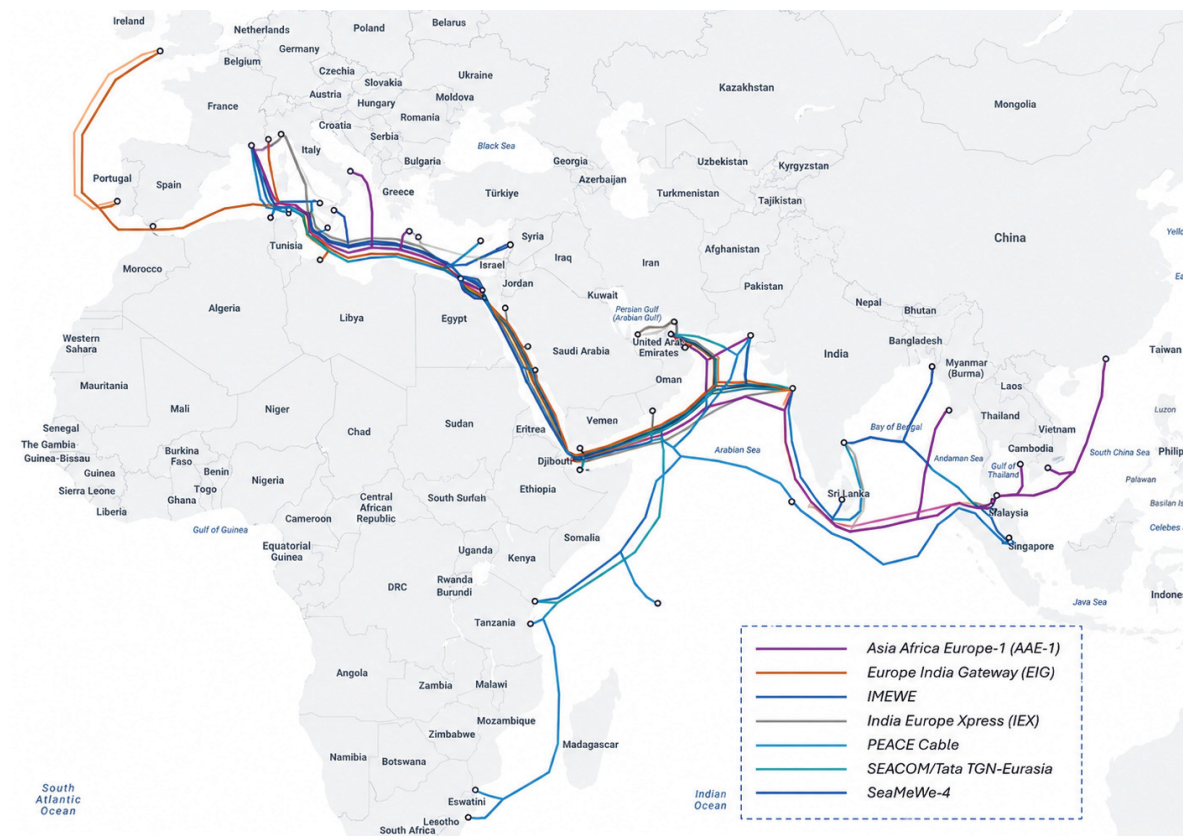
making Egypt arguably the most critical single-country chokepoint in the Euro-Mediterranean digital architecture (Murphy & Bryja, 2025). The operational cost of this dependence was illustrated in March 2025, when the PEACE cable was severed approximately 1,450 km from Zafarana and remained offline for nearly three months because repair vessels could not access the Red Sea conflict zone, replicating the access dynamics that had delayed AAE-1 repairs in 2024. Rerouting around the Cape of Good Hope lengthened transit times, raised fuel costs by over 30%, and sharply in-

creased war-risk insurance premium from 0.07% to as much as 2% of vessel value per transit (Moody, Tzourbakis, & Abdullahi, 2024). The strategic problem, as in the Indo-Pacific, lies not only in cable density but in the compression of critical routes into narrow, politically sensitive passages that are difficult to monitor, protect, and restore (Marchionna, 2025).

Figure 1 shows how AAE-1, EIG, SEA-COM, and India Europe Xpress cross a corridor shared by Greek, Cypriot, Turkish, Israeli, Lebanese, and Egyptian jurisdictions, many of them disputed. Offshore platforms and pipelines in the Levantine

Basin further complicate the picture by sharing the seabed with cable routes. In the Aegean, sustained naval posturing between Greece and Türkiye creates a persistent risk of miscalculation in which seabed infrastructure becomes a latent instrument of coercive leverage. The Central Mediterranean functions as the main connectivity bridge between Europe and North Africa, with cables linking Italy, Malta, Tunisia, Libya, and Algeria essential both for bilateral communication and for the EU's wider digital connectivity agenda, including emerging green hydrogen corridors and investments under the Global Gateway framework.

**Figure 1.** Submarine cable routes and landing stations along the Europe–Asia–Africa corridor, with detail of the Mediterranean basin, illustrating route concentration, contested jurisdictions, and principal chokepoints



Note. Sourced from TeleGeography, 2026.

## A threat typology

A useful framework for assessing risk distinguishes three analytical dimensions: the intentionality of the event, the threat category through which it operates, and the function targeted.

The same observed damage, a severed cable or an unreachable control system, may derive from very different causes, and ambiguity over intentionality is often itself a feature of hybrid strategy, as it raises the threshold for response. Four threat categories structure the analysis.

Deliberate physical sabotage has gained political salience since 2022, when repeated Baltic Sea incidents showed how quickly infrastructure damage can escalate into a high-level political event, even where coordinated intent remains unproven. This dynamic culminated in the December 2025 Fitburg incident, which severed a Helsinki-Tallinn fibre-optic line and triggered a national emergency response in Finland (Gratias, 2025; Jones, 2026).

A second growing category is cyber intrusion targeting port and maritime digital infrastructure, including GPS manipulation, espionage, and sabotage by state-linked actors: maritime cyber incidents rose from three in 2013 to 64 in 2023, and state-linked actors including Iranian APT groups - specialised units conducting long-term covert operations against targeted networks - have conducted operations involving GPS manipulation, espionage, and sabotage that could prove difficult to distinguish from physical attacks (Moody, Tzourbakis, & Abdullahi, 2024; Cyble Research and Intelligence Labs, 2025).

Accidental damage remains the most frequent cause of cable disruption globally,

with bathymetry a critical but under-appreciated variable: damage at 200 metres implies very different repair timelines than identical damage at 3,000 metres (ICPC, 2025; Minuto, 2026).

The fourth and most analytically difficult category is hybrid action, combining physical and cyber means whilst preserving deliberate ambiguity over origin and intent, illustrated by the Eastern Mediterranean GPS spoofing events of late 2023, in which over 100 vessels displayed false AIS positions near Beirut airport during the Gaza conflict. Across all four categories, the attack surface extends beyond the submerged segment to onshore nodes, supply chains, supervisory systems, and regulatory frameworks (ENISA, 2023; European Commission, 2025, 2026).

## The Red Sea fallout and the Hormuz dimension

Since November 2023, Houthi operations in the Red Sea have forced large volumes of commercial shipping to reroute around the Cape of Good Hope, increasing pressure on Mediterranean cable corridors through higher traffic density, disrupted repair logistics, and rising insurance costs (Fasulo et al., 2026). The September 2025 cuts to the SMW4 and IMEWE cables near Jeddah demonstrated how kinetic disruption in one corridor can generate digital degradation across interconnected systems (ComplexDiscovery, 2025).

By early March 2026, this dynamic had reached a new level of severity. Following US-Israeli strikes on Iran under Operation Epic Fury on 28 February 2026, the Islamic Revolutionary Guard Corps (IRGC) declared the Strait of Hormuz closed on 2 March, while Houthis resumed attacks on Red Sea shipping in support of Tehran,

Maritime cyber incidents rose from three in 2013 to 64 in 2023, and state-linked actors including Iranian APT groups have conducted operations involving GPS manipulation, espionage, and sabotage that could prove difficult to distinguish from physical attacks.

ending a ceasefire that had held since late 2025. For the first time in recorded history, both major maritime data choke-points linking Europe to Asia and Africa were simultaneously compromised, leaving the submarine cables transiting the Red Sea and the systems serving the Hormuz corridor effectively inaccessible to repair vessels (Hawkins, 2026).

These disruptions reinforce a wider European lesson: cable resilience depends on route redundancy, but also on industrial depth – the domestic capacity to manufacture, deploy, and maintain cable systems – repair readiness, and governance arrangements capable of anticipating crises before they cascade across connected corridors (Marchionna, 2025).

This is no longer simply a scenario to be modelled. It is the operational context within which European maritime security planners, telecommunications regulators, and naval commanders must now act.

## **From disruption to crisis: escalation pathways in the Mediterranean digital domain**

Cable cuts, port cyber incidents, and seabed confrontations do not escalate automatically. They escalate through the interaction of technical ambiguity, pre-existing political tensions, institutional fragmentation, and compressed response timelines. This section reconstructs the escalation logic through three empirical cases and then identifies the cross-cutting dynamics that make the Mediterranean structurally more volatile than other cable-dense regions. Aimed to isolate the conditions under which it does, and those under which it does not, the three cases that follow are selected for variation rather

than confirmation. They differ systematically along the four variables set out above, most clearly along the axis of intentionality, from unintended collateral damage (Vignette A), through action of contested origin (Vignette B), to a compound scenario unfolding amid open regional escalation (Vignette C), and across the basin's tiers, from the data-dense northern shore to the structurally thinner southern and eastern connectivity landscapes.

### **An escalation framework**

Four variables consistently shape whether a maritime digital disruption remains a manageable operational incident or develops into a political or military crisis.

The first is attribution ambiguity. A cable cut or a port cyber intrusion carries no clear return address, creating a window of uncertainty in which competing narratives proliferate and decision-makers must act on incomplete information. The Baltic Sea experience between 2022 and 2025 shows that, in nearly every major incident, weeks or months passed before even partial attribution emerged. In the November 2024 damage to BCS East-West Interlink and C-Lion1, the Chinese cargo vessel *Yi Peng 3* was identified as the probable cause, yet no definitive legal attribution was reached. German Federal Defence Minister Boris Pistorius publicly stated that accidental damage was not credible, but that political judgement did not translate into actionable legal or operational evidence (Wilson Center, 2025). Evidence from the Taiwan Strait and the Baltic Sea also suggests that, even where cable faults are frequent, proof of coordinated state-directed sabotage often remains limited, and that network redundancy, international norms, and the risk of political backlash may make deliberate sabotage less attractive as a grey-zone tactic than public narratives often assume (Gratias, 2025).

The second variable is pre-existing political tension. Incidents occurring against a background of existing interstate rivalry or geopolitical tension have far greater escalation potential than technically similar incidents in more stable settings, shaping whether an incident activates crisis management mechanisms, triggers defensive military repositioning, or is used for coercive signalling. Each of these outcomes carries a different escalation profile and requires a different institutional response.

The third variable is response timeline asymmetry. Cable repairs in the Mediterranean take weeks or months even under favourable conditions, a baseline further extended by the combination of adjacent conflict zones, contested jurisdictions, and the absence of pre-positioned repair capacity in the basin. Cyber incidents affecting port systems may paralyse operations for days before containment is achieved. Both dynamics create political pressure to act, compress decision cycles, and increase the risk of miscalculation. The implications are particularly serious for Command, Control, Communications, Computers and Intelligence (C4I). Naval operations increasingly depend on commercial fibre-optic infrastructure for data fusion and situational awareness. A cable disruption can therefore degrade Maritime Domain Awareness (MDA), the integrated real-time picture of activity across the maritime environment, as well as generate economic damage (NATO Review, 2024).

The fourth is the relationship between technical vulnerability and political leverage. High technical vulnerability does not automatically produce high political leverage

for the disruptor. The actual impact depends on the redundancy and reconfigurability available to the target. This asymmetry is especially pronounced in the Mediterranean's southern tier. Connectivity landscapes in North Africa and the Levant are structurally thinner than those of the northern shore, meaning that similar disruptions can carry much greater political weight. Analytical frameworks that treat all cable cuts as equivalent will therefore tend to misjudge escalation risk (Valeriani, 2026).

### **Vignette A - The Eastern Mediterranean: collateral damage, strategic consequences**

On 18 February 2024, the Belize-flagged<sup>17</sup> bulk carrier MV Rubymar was struck by two Houthi anti-ship ballistic missiles west of Hudaydah, abandoned with an unsecured anchor deployed, and drifted for 13 days before sinking on 2 March 2024. Its dragging anchor severed AAE-1, EIG, and SEACOM/TGN, disrupting approximately 25% of telecommunications traffic between Western Asia, North Africa, and Europe (Patil & Gupta, 2024). Repairs to AAE-1 were not completed until July 2024 - a five-month outage delayed by permit disputes and the near-impossibility of deploying repair vessels into an active conflict zone (Bloomberg, 2024). The incident is analytically significant not for what happened in the Red Sea but for what it revealed about downstream vulnerability: kinetic disruption in one corridor generates digital degradation in another without any direct attack on Mediterranean

Kinetic disruption in one corridor generates digital degradation in another without any direct attack on Mediterranean infrastructure.

<sup>17</sup> Belize-flagged vessels are registered with the International Merchant Marine Registry of Belize (IMMARBE), which accepts owners of any nationality. Recently, such vessels have been involved in maritime incidents, including the sinking of a dredger in Singapore (April 2025), damage to the Rubymar in the Red Sea (February 2024), and the grounding of the Felicity 8. See: Reuters, 2024; Solon & Hatem, 2024; U.S. Central Command, 2024.

infrastructure. This indirect escalation pathway - from a Houthi missile strike to C4I-relevant connectivity degradation at European landing stations - is precisely the kind of effect that existing threat assessment frameworks, calibrated primarily for direct attacks, are poorly equipped to anticipate (Galassi & Marchionna, 2024). Crucially, the cable damage was neither the object nor a foreseen consequence of the strike. The operational end goal of Houthi action was the interdiction of commercial shipping in support of the Gaza campaign and, through it, Tehran's regional signalling; the severing of AAE-1, EIG, and SEACOM/TGN was a second-order effect of an abandoned vessel's dragging anchor. It is this dissociation between intent and effect that defeats threat frameworks calibrated for purposive attack: the single most consequential disruption to Euro-Mediterranean connectivity in 2024 had no author who sought it.

### **Vignette B - The Central Mediterranean: port cyber events and the attribution trap**

The Central Mediterranean's cyber threat landscape has intensified significantly since 2023, with coordinated ransomware attacks on port infrastructure in Antwerp-Zeebrugge, Hamburg, and Ghent in late 2022, a DDoS attack on the Port of Rotterdam in June 2023, and targeted operations by the Iranian state-linked cyber actor Crimson Sandstorm against Mediterranean maritime sectors by 2025 (Austin et al., 2025; Cyble Research and Intelligence Labs, 2025). Three structural factors create a specific attribution trap. Ports in politically fragile states - notably Libya and Tunisia - present weak IT/OT governance and blurred lines between criminal, hacktivist, and state-linked activity. Cable landing stations in Sicily, Malta, Sardinia, and Tunisia serve simultaneously

as civilian telecommunications infrastructure and logistically important nodes for European Union (EU) naval operations, yet remain lightly protected (CSIS, 2024). GPS spoofing during the 2023 Gaza conflict, when over 100 vessels displayed false AIS positions near Beirut airport, adds a cyber-physical dimension that degrades the vessel traffic data underpinning Maritime Domain Awareness (MDA) (Diakun, 2024).

These events do not share a single motive: ransomware against the northern European ports pursued financial extortion; the Rotterdam DDoS was demonstrative; the spoofing off Beirut, occurring within an active conflict, served military deception. Observed from the targeted node, however, the three are initially indistinguishable, and a state-linked actor can deliberately shelter purposive action behind the ambient noise of criminal and hacktivist activity. The motive is not missing from the analysis, since its illegibility is the threat. The result is a recurring dilemma: governments must choose between overreacting to incomplete information or absorbing the disruption and signalling tolerance - the first risks turning a criminal incident into a diplomatic crisis, the second risks creating a permissive environment for further coercive action (Bassoli, 2025).

### **Vignette C - The Aegean and the Hormuz cascade: an escalation in progress**

The most consequential illustration of Mediterranean digital vulnerability is unfolding in real time. Following US-Israeli strikes on Iran under Operation Epic Fury on 28 February 2026, the IRGC declared the Strait of Hormuz closed on 2 March whilst the Houthis resumed attacks on Red Sea shipping. The closure bears on Mediterranean connectivity through the

Governments must choose between overreacting to incomplete information or absorbing the disruption and signalling tolerance, the first risks turning a criminal incident into a diplomatic crisis, the second risks creating a permissive environment for further coercive action.

logistics of cable restoration. Repair vessels cannot enter contested or closed waters, so the systems transiting the Gulf and the Red Sea become physically unreachable; and because the global cable-repair fleet is both finite and risk-averse, an active theatre absorbs the assets available across the entire Red Sea-Gulf arc, degrading restoration capacity well beyond the corridor actually in crisis. The decisive link between the two chokepoints, however, is financial: the withdrawal of P&I and war-risk cover for Hormuz transits on 5 March rendered repair operations uninsurable, and therefore unviable, even where damage had already occurred (Hawkins, 2026): restorability now depending on the London insurance market as much as on technical feasibility. For the first time in recorded history, both major maritime data chokepoints linking Europe to Asia and Africa were thus simultaneously compromised, with cables in both corridors effectively beyond repair.

In the Aegean, the relevant risk is jurisdictional rather than functional: energy and data infrastructure share the same contested seabed and the same exposure to naval interdiction. The Great Sea Interconnector, an HVDC power link, has faced repeated disruption since July 2024, when Türkiye deployed five warships to obstruct survey activity, and in August 2025 a Turkish naval frigate intercepted the survey vessel Fugro Gauss during preliminary work on the related EMC data cable, which shares its corridor and permitting path (Reuters, 2024; Qiu, 2025). What the interconnector episode reveals is the posture that would govern a data-cable incident in the same waters: the disputed seabed makes any survey, lay, or repair operation a potential trigger for naval confrontation, irrespective of whether the cable carries electrons or data.

The underlying dispute remains structurally unresolved, not least because Türkiye

has not ratified UNCLOS (SAIS Review of International Affairs, 2026). This structural contestation does not contradict the diplomatic rapprochement between Athens and Ankara underway since 2023: as Chapter 1 notes, the improved bilateral tone has not resolved the Eastern Mediterranean's underlying disputes. The détente operates at the level of high-level diplomacy, whereas the contested seabed remains governed by the delimitation question and the Mavi Vatan doctrine that diplomatic warming has left untouched. It is precisely this decoupling of political de-escalation above and structural contestation below that keeps subsea infrastructure a residual flashpoint even in a phase of improving relations. Under these conditions, a cable incident in the Eastern Mediterranean - whether accidental, collateral, or deliberate - would unfold in an environment where attribution is immediately contested, European naval assets are under pressure from the Red Sea and Hormuz, repair access is shaped as much by insurance markets as by technical feasibility, and North Atlantic Treaty Organization (NATO) cohesion is strained by an active territorial dispute between two member states bound to mutual defence: a contradiction internal to the Alliance that complicates any collective response and that other allies have strong incentives to avoid adjudicating. The pathway from incident to crisis is short, fast, and institutionally unmanaged.

## Cross-cutting dynamics

Read in sequence, three vignettes reveal patterns that recur across otherwise dissimilar incidents. Where the four variables above explain how a given incident escalates, the three cross-cutting dynamics below explain why the Mediterranean as a system is predisposed to such escalation, and together they define the Mediterranean's specific escalation profile.

European naval assets are under pressure from the Red Sea and Hormuz, repair access is shaped as much by insurance markets as by technical feasibility.

The first is the collapse of the civilian-military distinction. In all three cases, civilian infrastructure became either the object or the instrument of strategic signalling<sup>18</sup> and, crucially, it need not be the intended target to acquire strategic weight. Disruption propagates from the kinetic to the digital domain without any direct attack on the cable: an anchor dragged by a stricken or manoeuvring vessel, as off Jeddah in September 2025, or a corridor rendered uninsurable and thus beyond repair, as in the Hormuz-Red Sea convergence of 2026, where no cable need be touched for connectivity to collapse. The same severed cable is consistent with a negligent merchant vessel and with a ship disabled by hostile fire, leaving the event suspended between accident and attack. A disruption affecting civilian digital infrastructure is simultaneously a commercial disruption, a C4I degradation event, and a potential precursor to kinetic escalation, yet no unified institutional framework exists to assess and manage it as such (Dimitrova et al., 2025). NATO's Multi-Domain Operations doctrine depends on reliable and timely information flows across physical, informational, and cognitive domains, precisely what is degraded when cables are disrupted and AIS data manipulated. Yet a command-and-control architecture that lacks anticipatory integration across civilian and military domains remains structurally reactive (Blatny & Søndergaard, 2025; NATO, 2021). This gap is compounded by the threshold paradox: hybrid attacks are designed to remain below the threshold triggering a formal collective response, whilst any proportionate response would require procedures built for above-threshold crises, creating a pattern of absorption rather than deterrence (Valeriani, 2026).

The second is repair ecosystem fragility. Fewer than 60 vessels worldwide are capable of deep-sea cable repair, none are pre-positioned in the Mediterranean, and their deployment depends on insurance availability, port access, and the absence of active conflict zones (Armada International, 2025). The timelines seen in the Red Sea - five months for AAE-1 and three months for PEACE - should be treated as plausible baseline scenarios rather than exceptional outcomes. Investment continues to flow towards monitoring and early-warning systems whilst the more basic question of how many specialised vessels Europe can deploy at short notice remains insufficiently addressed, a gap that falls between EU regulatory frameworks, NATO operational planning, and national procurement cycles with no obvious institutional home (Faraday, 2026; Minuto, 2026; Oehlers, 2026). The global average of around 40 days between fault identification and service restoration is a window of strategic exposure during which an adversary can exploit degraded connectivity before restoration is achieved (Boschetti et al., 2025; European Commission, 2026).

The third is the absence of a shared risk vocabulary. Maritime authorities, telecom regulators, cybersecurity agencies, naval commands, and private insurers operate with different taxonomies, thresholds, and reporting logics, meaning that the same incident may be classified differently by each actor, producing contradictory interpretations and incompatible responses. The consequence is escalation risk: in the critical window after an incident, the absence of a shared classification means no actor can authoritatively fix what the event is (accident, crime, or attack) and

NATO's Multi-Domain Operations doctrine depends on reliable and timely information flows across physical, informational, and cognitive domains, precisely what is degraded when cables are disrupted and AIS data manipulated.

<sup>18</sup> Strategic signalling means the use of infrastructure incidents to communicate coercive intent below the threshold of armed conflict.

that interpretive vacuum is itself the space in which coercive ambiguity operates. When disruption forces emergency re-routing, the issue becomes not only technical but also political, as exposure shifts to alternative providers, jurisdictions, and regulatory systems (Minuto, 2026; Salamone, 2026; Valeriani, 2026). The result is a layered resilience deficit in which civilian, institutional, and military actors each maintain their own continuity arrangements without a common protocol for synchronising responses when disruption crosses sectors (Dimitrova et al., 2025).

### **The governance map: actors, mandates, and limits**

The actor's mandates were designed for separate domains and for conditions of normality, producing not a governance vacuum but a governance mosaic.

The governance challenge is not the result of absent actors - maritime authorities, telecommunications regulators, cybersecurity agencies, naval commands, and private infrastructure operators are all active across the Mediterranean. The problem is structural: their mandates were designed for separate domains and for conditions of normality, producing not a governance vacuum but a governance mosaic in which multiple overlapping authorities each hold partial visibility and none has the cross-domain mandate required to manage incidents that simultaneously cross physical, cyber, and geopolitical boundaries. Three functional clusters define the existing landscape. Surveillance and early warning - covering the International Maritime Organization (IMO), the European Maritime Safety Agency (EMSA), national cybersecurity agencies operating under NIS2, and the EU Cable Action Plan - stops at maritime boundaries and is designed for individual operators rather than cross-border crises (European Commission, 2025, 2026). Operational response, covering NATO's Maritime Centre for the Security of Critical

Undersea Infrastructure and national initiatives such as Italy's Law 9/2026, which empowers the Italian Navy to intercept vessels threatening submarine infrastructure of national interest, faces a legal and political ceiling: naval assets cannot unilaterally interdict civilian vessels in international waters without raising the very diplomatic risks that hybrid operations are designed to exploit (Triggiano, 2026). Data governance covering the EU's Common Information Sharing Environment (CISE) and private cable operators relies on voluntary participation and creates no general obligation to share operationally sensitive data beyond narrow incident-notification requirements. Each cluster, in other words, fails precisely where the corresponding cross-cutting dynamic bites: surveillance fragments along the same lines as the missing shared vocabulary, operational response runs into the threshold paradox, and data governance reproduces the layered resilience deficit at the institutional level. The governance mosaic is misaligned with the structure of the threat.

### **Key structural gaps**

Three structural gaps emerge from this governance map, and none can be closed by a single actor.

The first is the absence of cross-sector coordination protocols. No permanent mechanism connects maritime authorities, telecom regulators, cybersecurity agencies, naval commands, and private operators around a shared situational picture. As a result, inter-agency communication must be improvised under time pressure and across incompatible institutional vocabularies. The NIS2 and CER Directives impose resilience obligations, but they do not create operational channels linking cybersecurity authorities to the maritime and military actors who would need to

manage the physical dimension of a hybrid incident.

The second is jurisdictional ambiguity in international waters. Roughly 65% of submarine cables run through areas where no single state exercises full jurisdiction (Sari, 2025). Although Article 113 of United Nations Convention on the Law of the Seas (UNCLOS) obliges states to criminalise wilful damage to cables, grey-zone actors operate precisely in the space between the threshold for protective action and the threshold for legal certainty. In the Mediterranean, this problem is compounded by unresolved maritime claims and by Türkiye's non-ratification of UNCLOS, particularly in the Aegean and Eastern Mediterranean.

The third gap is the misalignment between public and private incentives, compounded by data opacity across the infrastructure chain. Private operators, hyperscalers, and repair contractors optimise for commercial continuity rather than strategic resilience, while the operational data required for cross-sector crisis coordination remains largely outside public reach. Hyperscalers now control a significant share of global subsea bandwidth yet are under no obligation to provide public authorities with data in forms usable for crisis management (Galassi & Marchionna, 2024). This opacity has operational consequences: restoration timelines reflect both technical constraints and the accumulated friction of contracting, permitting, insurance clearance, and restricted data access. Existing EU legislation provides a partial

basis for addressing this problem, but current arrangements still fall short of creating meaningful data-sharing obligations proportionate to the strategic relevance of the infrastructure. Existing EU legislation offers part of the legal basis for improvement, but current arrangements or emerging proposals of structured models of risk-based data access and reciprocal transparency, like AGOR and CTR,<sup>19</sup> still do not resolve the underlying tension between cross-border data sharing and national informational sovereignty, especially in periods of acute geopolitical stress. That tension is a problem of governance design, and one that the policy instruments proposed in the next section must confront directly.

## Conclusions and Recommendations

The Mediterranean's submarine cable system is a strategic resilience challenge at the intersection of maritime security, digital continuity, and geopolitical competition. The region's vulnerability derives not only from the physical exposure of cables and landing stations, but from the interaction between infrastructure concentration, attribution ambiguity, and fragmented governance.

Three conclusions follow. First, the Mediterranean is structurally exposed because it combines dense cable corridors, unresolved maritime disputes, and fragile repair arrangements. Second, escalation risk depends less on the

Restoration timelines reflect both technical constraints and the accumulated friction of contracting, permitting, insurance clearance, and restricted data access.

<sup>19</sup> AGOR (in Italian *Apertura Graduata Orientata al Rischio*) means Risk-Oriented Gradual Opening, a risk-based system for classifying infrastructure data across graduated access tiers. CTR (in Italian *Contratto di Trasparenza Reciproca*) means Mutual Transparency Agreement, a contractual mechanism establishing reciprocal transparency obligations between public authorities and private operators. See: Triggiano, A. (2026). Per una protezione integrata dei cavi sottomarini: La legge n. 9/2026 alla prova di un paradigma data-oriented. Astrid Rassegna, 5/2026.

number of incidents than on the absence of shared mechanisms to classify, notify, and manage them. Third, resilience depends not only on surveillance or deterrence, but on continuity across the full infrastructure chain. Two practical instruments can help operationalise this approach.

**Artifact 1 – Minimum resilience baseline**

The following baseline (Table 1) translates resilience into a minimum set of practical measures applicable across EU member states and Mediterranean partner countries.

**Table 1.** Minimum measures applicable across EU member states and Mediterranean partner countries

| Priority Area              | Minimum Requirement                                                                                                                         | Operational Purpose                                               |
|----------------------------|---------------------------------------------------------------------------------------------------------------------------------------------|-------------------------------------------------------------------|
| Redundancy                 | Map critical dependencies and ensure at least one fallback path for essential government, financial, emergency, and security communications | Reduce single points of failure                                   |
| Segmentation               | Separate priority traffic from bulk commercial flows and define service-restoration priorities in advance                                   | Protect continuity of essential functions                         |
| Continuous Monitoring      | Establish integrated monitoring of cable routes, landing stations, and anomalous vessel activity near critical nodes                        | Shorten the gap between anomaly detection and coordinated action  |
| Landing-Station Protection | Apply minimum physical security, backup power, access control, and cyber-hardening standards at landing stations                            | Protect the most accessible and operationally consequential nodes |
| Repair Readiness           | Pre-arrange repair contracts, customs fast tracks, port access, spare-part stocks, and escort/support procedures for repair windows         | Reduce restoration delays during crises                           |
| Exercises and Contacts     | Maintain updated 24/7 contact chains and conduct recurring joint exercises involving operators, coast guards, cyber agencies, and navies    | Build trust and operational familiarity before incidents occur    |

Note. Elaborated by the author, sourced from Lons (2026).

This baseline should be understood as a resilience floor, instead of an aspirational standard. Its value lies in establishing a minimum posture across prevention, detection, response, and restoration, while giving the EU a practical framework for technical support to Mediterranean partner countries.

## Artifact 2 – 72-hour crisis Playbook

The following Playbook (Table 2) provides a simple decision structure for the first 72 hours after a major cable incident, when early coordination is critical to containing escalation.

**Table 1.** 72-hour Crisis Playbook for major cable incidents

| Phase                                                           | Actions                                                                                                                                                                                                                                                                                                                                                                                                                                                                          | Actors                                                      | Objective                                                                             |
|-----------------------------------------------------------------|----------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|-------------------------------------------------------------|---------------------------------------------------------------------------------------|
| <b>0–6 hrs.</b><br><br><b>Detect, Notify, Classify</b>          | <ul style="list-style-type: none"> <li>▪ Detect anomaly and trigger immediate notification</li> <li>▪ Alert maritime authorities, telecom regulators, cyber agencies, and naval commands simultaneously</li> <li>▪ Provisionally classify incident as: unconfirmed / suspected accidental / suspected malicious / indeterminate</li> </ul>                                                                                                                                       | Operators, EMSA, ENISA, national cyber agencies             | Shared awareness without premature attribution                                        |
| <b>6–24 hrs.</b><br><br><b>Stabilise, Protect, Preserve</b>     | <ul style="list-style-type: none"> <li>▪ Activate cross-sector coordination cell</li> <li>▪ Reroute priority traffic and secure essential communications</li> <li>▪ Protect adjacent cable routes and landing stations</li> <li>▪ Preserve AIS, radar, OT, and operator logs for later attribution</li> <li>▪ Shadow, inspect, or interdict suspicious vessels where legally feasible</li> </ul>                                                                                 | Naval commands, coast guards, operators, cyber agencies     | Contain operational impact and prevent escalation through institutional fragmentation |
| <b>24–72 hrs.</b><br><br><b>Deconflict, Repair, Communicate</b> | <ul style="list-style-type: none"> <li>▪ Activate deconfliction channels in contested or politically sensitive waters</li> <li>▪ Launch protected repair preparation, including access permissions, customs clearance, and maritime safety arrangements</li> <li>▪ Centralise public messaging on what is known, what remains uncertain, and what continuity measures are in place</li> <li>▪ Withhold definitive attribution until the technical picture has matured</li> </ul> | Diplomatic channels, repair contractors, public authorities | Preserve restoration space whilst limiting the political risks of misperception       |
| <b>CROSS-CUTTING</b><br><br><b>Safe Repair Understandings</b>   | <ul style="list-style-type: none"> <li>▪ Emergency notification of repair missions</li> <li>▪ Non-interference commitments for certified repair vessels</li> <li>▪ Technical hotlines among competent authorities</li> <li>▪ Expedited access and permit procedures during crisis periods</li> </ul>                                                                                                                                                                             | All actors                                                  | Protect the technical restoration process across all phases                           |

Note. Elaborated by author.

The logic of this Playbook is straightforward: stabilise first, accuse later. A shared schematic of this kind would help reduce uncertainty at the precise moment when political pressure is highest and technical clarity remains limited.

Its main value lies in imposing discipline across sectors that normally operate with different timelines, mandates, and risk vocabularies. The actors involved need a common sequence of action during the initial crisis window. The Safe Repair Understandings are particularly important in this respect: their purpose is to ensure that during a defined emergency window, bona fide repair missions are not obstructed, harassed, or militarised, even in sensitive waters, a narrowly practical confidence-building measure that requires no prior political agreement to implement. It is precisely the operational utility without the precondition of political consensus that makes the Safe Repair Understandings a candidate for elevation from an ad hoc crisis practice to a standing diplomatic instrument, as set out in the institutional recommendations below.

### Institutional recommendations

Three institutional priorities follow directly from this analysis. These recommendations build on an institutional architecture already in place. The EU Action Plan on Cable Security (2025), the EU-wide risk assessment of October 2025, and the Cable Security Toolbox and 13 Cable Projects of European Interest of February 2026 span the full resilience cycle and apply to all EU sea basins (European Commission, 2025, 2026). Implementation, however, has begun in the Baltic, where the concentration of incidents between 2023 and 2025 drove both the pilot funding and the priority basin for the CEF Digital call on pre-positioned repair modules. The Mediterranean extension,

planned from 2026, must contend with conditions absent from the Baltic theatre: contested chokepoints, partner-country dependencies, and frictions between allied states sharing the same disputed waters. The priorities below translate the existing EU effort into terms adapted to the basin.

First, **NATO** should strengthen the Maritime Centre for the Security of Critical Undersea Infrastructure with a specific Mediterranean mandate. The Baltic incident record offers relevant lessons on attribution, response coordination, and political signalling, but the Mediterranean presents a distinct combination of chokepoints, partner-country dependencies, unresolved jurisdictional disputes, and intra-alliance frictions that require dedicated scenario planning and stronger civil-military liaison.

Second, the EU should integrate cable incident reporting into the Common Information Sharing Environment (**CISE**). Without a shared maritime information layer covering cable disruption, suspicious activity near routes, and repair status, national authorities will continue to operate through fragmented sectoral channels. The EU's coordinated maritime presences, trialled in the Gulf of Guinea and the North-Western Indian Ocean (see Chapter 1, this volume), offer a light-footprint model directly transferable to the monitoring of Mediterranean cable nodes, pooling situational awareness without permanently stationed forces.

Third, the **EU and Mediterranean partners** should establish a diplomatic framework for subsea confidence-building measures through existing formats such as the 5+5 Dialogue and the Union for the Mediterranean (UfM). The Safe Repair Understandings introduced in the Playbook should form the operational core of such

a framework: as a narrowly bounded, technically framed commitment to leave bona fide repair missions unobstructed during defined emergency windows, they are implementable even where broader political agreement is absent – precisely

the condition that prevails in the most exposed Mediterranean waters, from the Aegean to the Levantine Basin. Around this core, the framework can layer the complementary arrangements the crisis window requires: notification protocols, emergency technical channels, and safe repair understandings during crises.

In 2026, with the principal digital choke-points connecting Europe to Asia and

Africa simultaneously under severe pressure, and with geopolitical tensions at their highest level in decades, the window for building even these minimum arrangements is narrowing rapidly. The central challenge is therefore to move from reactive vulnerability to proactive resilience, combining route diversification, repair readiness, and a shared operating picture across civilian, regulatory, and military actors.

The real test of resilience today is not only whether the region can protect its physical infrastructure, but whether it can develop the institutions needed to govern existing infrastructure effectively before the next disruption becomes a wider crisis.

## References

- AUSTIN, J., DAVYDIUK, A., DOLLIMORE, A., KAJANDER, A., & KURSETGJERDE, E. (2025). *Policy Brief Addressing State-Linked Cyber Threats to Critical Maritime Port Infrastructure*. [Policy brief]. NATO Cooperative Cyber Defence Centre of Excellence (CCDCOE). [https://ccdcoe.org/uploads/2025/07/CCDCOE\\_Policy\\_Brief.pdf](https://ccdcoe.org/uploads/2025/07/CCDCOE_Policy_Brief.pdf)
- BASSOLI, A.M. (2025, October 24). NATO's subsea cable strategy turns into a catch-22. *RealClearDefense*. [https://www.realcleardefense.com/articles/2025/10/24/natos\\_subsea\\_cable\\_strategy\\_turns\\_into\\_a\\_catch-22\\_1142966.html](https://www.realcleardefense.com/articles/2025/10/24/natos_subsea_cable_strategy_turns_into_a_catch-22_1142966.html)
- BODY OF EUROPEAN REGULATORS FOR ELECTRONIC COMMUNICATIONS (BEREC). (2024). *BEREC report on the general authorisation and related frameworks for international submarine connectivity*. BEREC. <https://www.berec.europa.eu/en/document-categories/berec/reports/berec-report-on-the-general-authorisation-and-related-frameworks-for-international-submarine-connectivity>
- BLATNY J. M., & SØNDERGAARD, S. (2025,). *Cognitive Warfare*. NATO Chief Scientist's Reports. NATO Science and Technology Organization. <https://www.sto.nato.int/document/cognitive-warfare/>
- BOSCHETTI, N., KOYYADA, A., DOWNS, B., ROSENTHAL, W., GORDON, N., LI-WÅNG, H., MARDER, A., SIGHOLM, J., FRÅNBERG, O., KINDGREN, J., FRISK, T., MAGNÚSSON, B. M., DUNN CAVELTY, M., JOHNSON, H., & FALCO, G. (2025). *Hybrid space and submarine architecture to ensure information security of telecommunications* (HEIST). IEEE Access. <https://ieeexplore.ieee.org/document/11237089>
- COMPLEXDISCOVERY. (2025, September 10). Red Sea cable cuts disrupt connectivity and expose global infrastructure risks. *ComplexDiscovery*. <https://complexdiscovery.com/red-sea-cable-cuts-disrupt-connectivity-and-expose-global-infrastructure-risks/>
- CYBLE RESEARCH AND INTELLIGENCE LABS. (2025, July 29). *Cyber threats surge against maritime industry in 2025*. <https://cyble.com/blog/cyberattacks-targets-maritime-industry/>
- CYDOME. (2026). *Maritime cyber trends report 2026: What shipping executives need to know*. Cydome. [https://cydome.io/cydome-maritime-trends-report-2026/?\\_gl=1\\*1rlqtdf\\*\\_up\\*MQ..\\*\\_ga\\*MzAwMzQ2MzEwLjE3Nzc5NjY2MDQ.\\*\\_ga\\_TNCE0XZNGB\\*czE3Nzc5NjY2MDQkbzEkZzEkdDE3Nzc5NjY2MDQkajYwJGwwJGgw](https://cydome.io/cydome-maritime-trends-report-2026/?_gl=1*1rlqtdf*_up*MQ..*_ga*MzAwMzQ2MzEwLjE3Nzc5NjY2MDQ.*_ga_TNCE0XZNGB*czE3Nzc5NjY2MDQkbzEkZzEkdDE3Nzc5NjY2MDQkajYwJGwwJGgw)
- DIAKUN, M. (2024). *War-zone location jamming sees more ships show up at airports*. *Lloyd's List*. Lloyd's List. <https://www.lloydslist.com/LL1148748/War-zone-GPS-jamming-sees-more-ships-show-up-at-airports>

DIMITROVA, D., MALVALEHTO, J., LOSADA, P., DAVIDSON, J., GALVAN, G., & BARRROWS, C. (2025). *Securing the underwater domain: Part 1 of 2 – Europe's underwater security is more critical and fragmented than ever before [White paper]*. Boston Consulting Group. <https://media-publications.bcg.com/Securing-the-Underwater-Domain-Part-1.pdf>

EKATHIMERINI. (2025, June 13). ADMIE seeks compensation over delays to €1.9 billion power-link project. *Ekathimerini*. <https://www.ekathimerini.com/economy/energy/1272252/admie-seeks-compensation-over-delays-to-e1-9-billion-power-link-project/>

EUROPEAN COMMISSION. (2025). *Joint communication of the Commission and the High Representative: EU action plan on cable security*. European Commission. <https://eur-lex.europa.eu/legal-content/EN/TXT/HTML/?uri=CELEX:52025JC0009>

EUROPEAN COMMISSION. (2026). *Security and resilience of EU submarine cable infrastructures: Submarine cable security toolbox and cable projects of European interest*. European Commission Expert Group on Submarine Cable Infrastructures. <https://digital-strategy.ec.europa.eu/en/library/submarine-cable-security-toolbox-and-cable-projects-european-interest>

EUROPEAN PARLIAMENT AND COUNCIL OF THE EUROPEAN UNION. (2022a). *Directive (EU) 2022/2555 on measures for a high common level of cybersecurity across the Union (NIS2 Directive)*. <https://eur-lex.europa.eu/eli/dir/2022/2555/oj/eng>

EUROPEAN PARLIAMENT AND COUNCIL OF THE EUROPEAN UNION. (2022b). *Directive (EU) 2022/2557 on the resilience of critical entities (CER Directive)*. <https://eur-lex.europa.eu/eli/dir/2022/2557/oj/eng>

EUROPEAN UNION AGENCY FOR CYBERSECURITY. (2023). *Undersea cables – what is at stake*. ENISA. <https://www.enisa.europa.eu/publications/undersea-cables>

FASULO, F., MISSAGLIA, N., & TALBOT, V. (Eds.). (2026). *IMEC: The backbone of an Indo-Mediterranean region. Italy and the future of transcontinental connectivity*. ISPI. [https://www.ispionline.it/wp-content/uploads/2026/03/Report-IMEC-2026\\_ISPI.pdf](https://www.ispionline.it/wp-content/uploads/2026/03/Report-IMEC-2026_ISPI.pdf)

FARADAY, E. (2025, December). *The Curran Papers—No. 4: Undersea cables: Strategic vulnerabilities and defence implications*. Armada International.

GALASSI, A., & MARCHIONNA, G. G. (2024). *Submarine cables and Mediterranean security: A governance gap analysis (LUISS School of Government Working Paper Series WP 3/2024)*. LUISS University Press. <https://sog.luiss.it/sites/sog.luiss.it/files/galassi.pdf>

GHOBARI, M.. (2024, March 2). Ship sunk by Houthis threatens Red Sea environment, shipping route. *Reuters*. <https://www.reuters.com/world/freighter-rubymar-has-sunk-red-sea-yemen-internationally-recognised-government-2024-03-02/>

GRATIAS, N. C. (2025). *Submarine cables and Chinese gray zone operations: Assessing alleged sabotage in the Taiwan Strait and Baltic Sea* [Master's thesis, Naval Postgraduate School]. <https://hdl.handle.net/10945/74816>

HAWKINS, N. (2026, March 5). Iran-US war puts subsea cable network on a knife-edge. *CapacityGlobal*. <https://capacityglobal.com/news/iran-us-war-subsea-cables-threat/>

INTERNATIONAL CABLE PROTECTION COMITEE. (2025, 16 May). *Media Enquiries & Frequently Asked Questions*. <https://www.iscpc.org/news/media-enquiries/>

INTERNATIONAL MARITIME ORGANIZATION (IMO). (2025). *MSC-FAL.1/Circ.3/Rev.3: Guidelines on maritime cyber risk management*. IMO. <https://wwwcdn.imo.org/localresources/en/OurWork/Security/Documents/MSC-FAL.1-Circ.3-Rev.3.pdf>

INTERNATIONAL ORGANIZATION FOR STANDARDIZATION. (2019). *ISO 22301:2019 security and resilience – Business continuity management systems*. ISO. <https://www.iso.org/standard/75106.html>

IOANNIDIS, S. (2025, September 1). Military prepares for any Turkish reaction to Cyprus power connection project. *eKathimerini*. <https://www.ekathimerini.com/politics/foreign-policy/1279452/military-prepares-for-any-turkish-reaction-to-cyprus-power-connection-project/>

JONES, B. D. (2026, February 13). Seabed zero: Baltic sabotage and the global risks to undersea infrastructure. *Bulletin of the Atomic Scientists*. <https://thebulletin.org/2026/02/seabed-zero-baltic-sabotage-and-the-global-risks-to-undersea-infrastructure/>

LINDHOLM, R. (2025). *Mapping undersea infrastructure attacks in the Baltic Sea*. Wilson Center. <https://www.wilsoncenter.org/article/mapping-undersea-infrastructure-attacks-baltic-sea>

MARCHIONNA, G. G. (2025). Submarine networks and maritime security in the Indo-Pacific: A strategic imperative to protect the invisible backbone of the EU's digital future. In M. Fink & A. Mishra (Eds.), *European perspectives on maritime security in the Indo-Pacific* (Panorama 2025/Issue 1, pp. 81–94). Konrad-Adenauer-Stiftung. <https://www.kas.de/en/web/politikdialog-asien/panorama/detail/-/content/european-perspectives-on-maritime-security-in-the-indo-pacific>

MINUTO, M. M. (2026, February 27). Interview by Gianmarco Gabriele Marchionna, Rome.

MOODY, E., TZOURBAKIS, S., & ABDULLAHI, K. (2024). *Ansar Allah and maritime security risks in the Red Sea*. Middle East Institute Switzerland. [https://meiswitzerland.ch/images/pdf/Red\\_Sea\\_report.pdf](https://meiswitzerland.ch/images/pdf/Red_Sea_report.pdf)

MURPHY, E. L., & BRYJA, T. (2025). *The strategic future of subsea cables: Egypt case study*. Center for Strategic and International Studies.

<https://www.csis.org/analysis/strategic-future-subsea-cables-egypt-case-study>

NATO. (2024). *Reinforcing resilience: NATO's role in enhanced security for critical undersea infrastructure*. NATO Review.

NATO. (2021). *Warfighting capstone concept*. NATO.

<https://www.act.nato.int/our-work/nato-warfighting-capstone-concept/>

NATO. (2023). *Baseline requirements for the protection of critical undersea infrastructure*. NATO.

PATIL, S., & GUPTA, P. (2024). *Red Sea crisis and submarine cables: Navigating uncharted waters*. Observer Research Foundation. <https://www.orfonline.org/expert-speak/undersea-chokepoints-the-red-sea-cable-disruptions>

QIU, W. (2014, January 31). *AAE-1 cable consortium inks construction and maintenance agreement*. SubmarineNetworks.

<https://www.submarinenetworks.com/en/systems/asia-europe-africa/aae-1/aae-1-cable-consortium-inks-construction-and-maintenance-agreement>

QIU, W. (2016, February 5). *AAE-1 consortium selects Xtera for equipping terrestrial segments*. SubmarineNetworks. <https://www.submarinenetworks.com/en/systems/asia-europe-africa/aae-1/aae-1-consortium-selects-xtera-for-equipping-terrestrial-segments>

QIU, W. (2025, August 13). *Turkey halts East Med Corridor cable survey*. SubmarineNetworks. <https://www.submarinenetworks.com/en/systems/asia-europe-africa/emc/turkey-block-survey-ship-for-east-to-med-corridor-cable>

QUATTROPANETTI, V. (2026, February 27). *La Marina Italiana guida la protezione delle infrastrutture critiche subacquee europee*. CyberSecurity Italia.

<https://www.cybersecitalia.it/la-marina-italiana-guida-la-protezione-delle-infrastrutture-critiche-subacquee-europee/60218/>

REUTERS. (2024, September 21). Cyprus signs MoU with Greece on “world’s longest” subsea electricity cable. *Reuters*. <https://www.reuters.com/business/energy/cyprus-signs-mou-with-greece-worlds-longest-subsea-electric-cable-2024-09-21/>

SAIS REVIEW OF INTERNATIONAL AFFAIRS. (2026). *Rethinking equitable maritime delimitation between Türkiye and Greece*. SAIS Review of international affairs.

<https://saisreview.sais.jhu.edu/rethinking-equitable-maritime-delimitation-between-turkiye-and-greece/>

SALAMONE, L. V. M. (2026, February 24). Vi spiego il potere delle infrastrutture invisibili. *Formiche.net*. <https://formiche.net/2026/02/vi-spiego-il-potere-delle-infrastrutture-invisibili-scrive-salamone-asi/>

SARI, A. (2025). *Protecting maritime infrastructure from hybrid threats: Legal options*. Hybrid CoE Research Report 14. Hybrid CoE. <https://www.hybridcoe.fi/publications/hybrid-coe-research-report-14-protecting-maritime-infrastructure-from-hybrid-threats-legal-options/>

SOLON, O., & HATEM, M. (2024, March 6). *Rubymar anchor seen as likely cause of severed Red Sea cables*. gCaptain. <https://gcaptain.com/rubymar-anchor-seen-as-likely-cause-of-severed-red-sea-cables/>

SOLON, O., & HATEM, M. (2024, July 17). Damaged Internet Subsea Cables Repaired in Red Sea Amid Militant Attacks on Ships. *Bloomberg*. <https://www.bloomberg.com/news/articles/2024-07-17/damaged-internet-cables-repaired-in-red-sea-as-houthis-attack-ships>

TELEGEOGRAPHY. (2026). *Submarine cable map* [Interactive map]. Retrieved 9 April, 2026, from <https://www.submarinecablemap.com/>

TRIGGIANO, A. (2026). *Per una protezione integrata dei cavi sottomarini: La legge n. 9/2026 alla prova di un paradigma data-oriented*. Astrid Rassegna 5/2026.

US CENTRAL COMMAND. (2024). *Sinking of motor vessel Rubymar risks environmental damage* [Press release]. U.S. Central Command. <https://www.centcom.mil/MEDIA/PRESS-RELEASES/Press-Release-View/Article/3693370/sinking-of-motor-vessel-rubymar-risks-environmental-damage/>

VALERIANI, M. (2026, February 27). Interview by Gianmarco Gabriele Marchionna, Rome.

WALL C., & MORCOS, P. (2021). *Invisible and vital: Undersea cables and transatlantic security*. Center for Strategic and International Studies. <https://www.csis.org/analysis/invisible-and-vital-undersea-cables-and-transatlantic-security>

WINDWARD MARITIME AI. (2026, March 1). *GPS jamming disrupts 1,100 ships in the Middle East Gulf*. Windward. <https://windward.ai/blog/gps-jamming-disrupts-1100-ships-in-the-middle-east-gulf/>

# **The Blue Data Bridge: Federated AI for Maritime De-securitisation**

**Elaine Donderer**

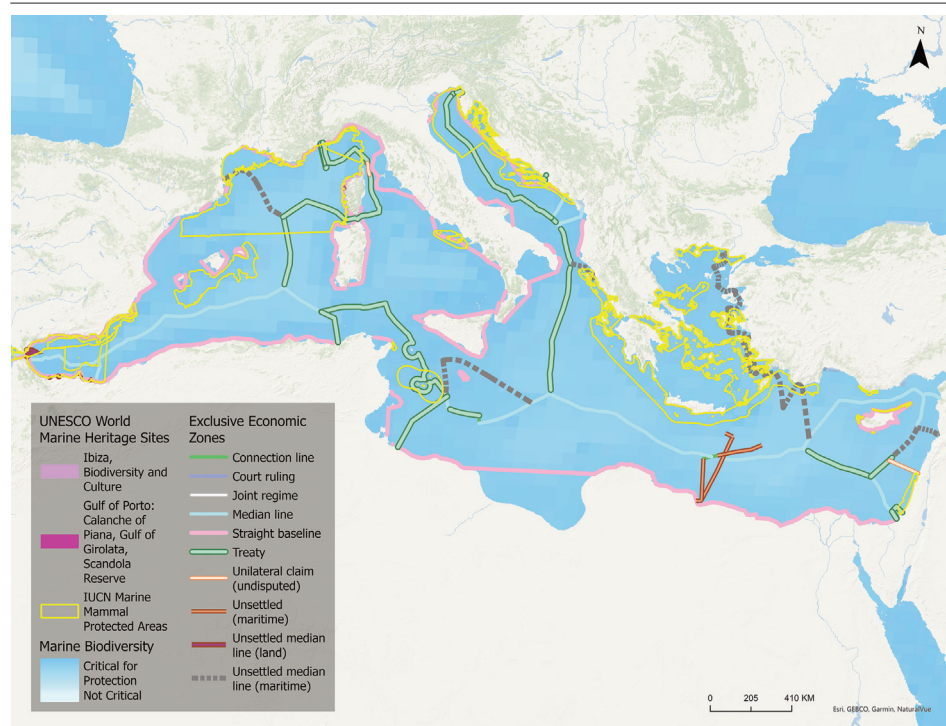
Consultant with the Arava Institute of Environmental  
Studies

## Introduction

The EU Maritime Security Strategy (EUMSS) Action Plan emphasises the need for a plug-and-play<sup>20</sup> information environment (European Union Maritime Security Strategy, 2014). The July 2024 launch of the European Union (EU)'s Common Information Sharing Environment (CISE) Operational Phase marks a transition from centralised, curated information toward more live information exchange and collective situational awareness within the Mediterranean (European Maritime Safety Agency, n.d.; Kapidani

et al., 2022). However, considerable amounts of data in the diverse maritime landscapes of the Mediterranean reside within public authority networks or on private server structures of port operators, shipping lines, cable owners, dive shops, and many more (Schaap et al., 2023). As illustrated in the previous chapter, this, in part, is due to the high prices of raw data and large computational loads of data transfer, but more often the lack of data sharing goes back to privacy and security concerns (Interview with Dr. Anita Graser, thematic coordinator at the Austrian Institute of Technology [AIT]).

**Figure 1.** Map of boundaries, biodiversity, and protection in the Mediterranean



Note. Elaborated by author, Elaine Donderer, 2026. The visualized data is based on the following sources: Flanders Marine Institute (2023). Maritime Boundaries Geodatabase, version 12. Available online at <https://doi.org/10.14284/628>, IUCN MMPATF (2025) Global Dataset of Important Marine Mammal Areas (IUCN IMMA). April 2026. Made available under agreement on terms and conditions of use by the IUCN Joint SSC/WCPA Marine Mammal Protected Areas Task Force and accessible via the IMMA e-Atlas <https://marinemammalhabitat.org/imma-eatlas/>, National Geographic Pristine Seas (2026). Marine Biodiversity. ArcGIS Imagery layer. Available online at [https://tiledimageservices.arcgis.com/P3ePLMYs2RVChkXj/arcgis/rest/services/210923e\\_biodiversity\\_ranking\\_WM\\_1000\\_masked\\_mrf\\_lerc/ImageServer](https://tiledimageservices.arcgis.com/P3ePLMYs2RVChkXj/arcgis/rest/services/210923e_biodiversity_ranking_WM_1000_masked_mrf_lerc/ImageServer)

<sup>20</sup> "Plug-and-play" refers to a principle whereby technical devices or systems can connect and operate seamlessly upon connection and without manual configuration.

Particularly in areas characterised by geopolitical sensitivities, security considerations may influence the extent and nature of voluntary data sharing, structurally undermining the completeness of regional information frameworks (Boustros, 2018; Interview with regional environmental governance expert). This lack of transparency has real costs, for instance, by driving up insurance premiums, delaying emergency responses, and increasing the risk of naval miscalculation. In 2025 alone, geopolitical friction and Houthi-led disruptions caused a 30% surge in global freight rates, and costs of up to \$1 million per rerouted voyage, affecting 12% of global shipping while spiking carbon emissions and insurance premiums (Berman, 2024; Kumar, 2026; Rai, 2025; Szentivanyi, 2024). Hence, the Mediterranean is no longer a theatre of purely kinetic naval competition but is characterised by a complex interplay of fragmented non-state actors, heterogeneous digital infrastructure, and untransparent supply chain logistics (Di Peri & Meier, 2023; Ehteshami & Mohammadi, 2017; Kapidani et al., 2022).

The Mediterranean is a vital transit hub for oil and gas destined for the EU and the United States (US) markets from other seas (Arvis et al., 2019). Additionally, the discovery of gas fields off the coasts of Israel, Cyprus, and Egypt has played its role in regional interests and tensions (Di Peri & Meier, 2023). Rather than a connecting bridge, the framing of the Mediterranean Sea through a narrow national security lens has historically reinforced divisions across continental, cultural, and political lines (Di Peri & Meier, 2023; Ehteshami & Mohammadi, 2017). The rising economic and military presence of major regional and global players, and their differing approaches towards the Mediterranean, further added to the securitisation and heterogeneous cartography of the space (Figure 1) (Di Peri & Meier, 2023; Ehteshami & Mohammadi, 2017; Kinacioglu, 2023).

While the prioritisation of military security in the Mediterranean mirrors dynamics in other highly contested chokepoints such as the Black Sea, the Red Sea, or the South China Sea, it shapes the urgency of European maritime policy (Germond, 2015). The securitisation of the maritime domain often takes precedence over other national and regional priorities such as blue economic growth or marine health preservation (Germond, 2015; Kinacioglu, 2023). Although militarised response strategies to these challenges remain routinised and prominent, they often fail to address, if not exacerbate, the underlying security dilemma.

Sustainable maritime security is a function of institutional trust, not unilateral surveillance. Transitioning the Mediterranean from a posture of reactive threat detection to one of decentralised, interconnected data governance transforms regional neighbours into security partners (Mitzen, 2006). Policy-makers have already started down this road when the European Commission and the High Representative issued a Pact to step up cooperation and economic connections across the Mediterranean Sea. With both EU and non-EU countries having Mediterranean coasts, the transnational nature of maritime security policy is evident (Figure 1). Countries share issues and challenges, such as the possible exploitation of submarine natural gas and oil resources, and the need for environmental conservation and planning. Healthy marine ecosystems are a central asset for coastal tourism and fishing industries and are both relevant and significant economic activities for the Mediterranean (European Union Maritime Security Strategy, 2014; European Commission, n.d.-a; The European Ocean Pact, 2025; Hogg et al., 2024).

To address these shared vulnerabilities, this policy brief advocates for strengthened historical, cultural, and multilateral ties to

outline a resilient, interconnected Mediterranean information framework. In complementing ongoing efforts, this analysis proposes that the European Maritime Safety Agency (EMSA) leverages privacy-preserving Federated Learning as an integral component of marine security policy. This helps foster a regional security community built on a shared, verified data truth rather than unilateral naval posturing. Grounded in empirical insights from six expert interviews with academics and environmental monitoring practitioners, as well as a semi-structured literature review to:

- a) Quantify Ghost Costs: Analyse common environmental and security risks and associated costs derived from incomplete information.
- b) Find Common Interests: Showcase three cases in which transboundary pressures, such as marine accidents, oil spills, and climate change, require a shared regional data truth.
- c) Pilot Privacy-Preserving Artificial Intelligence (AI): Define the technical requirements and system architecture for a Federated Learning module within the EU server networks to share environmental insights across the Mediterranean Sea.
- d) Blue Desecuritisation Framework: Draft a roadmap for sharing environmental data intelligence to incentivize regional maritime diplomacy, allowing for cooperation in contested waters where formal dialogue is stalled.

Beyond security, the Blue Data Bridge developed in this chapter demonstrates that

shared situational awareness is an economic and social prerequisite for a stable and sustainable future of the Mediterranean.

## **Federated Learning and Environmental Cooperation in the Mediterranean - A Path to Security?**

### **Insecurity at sea - and its cost**

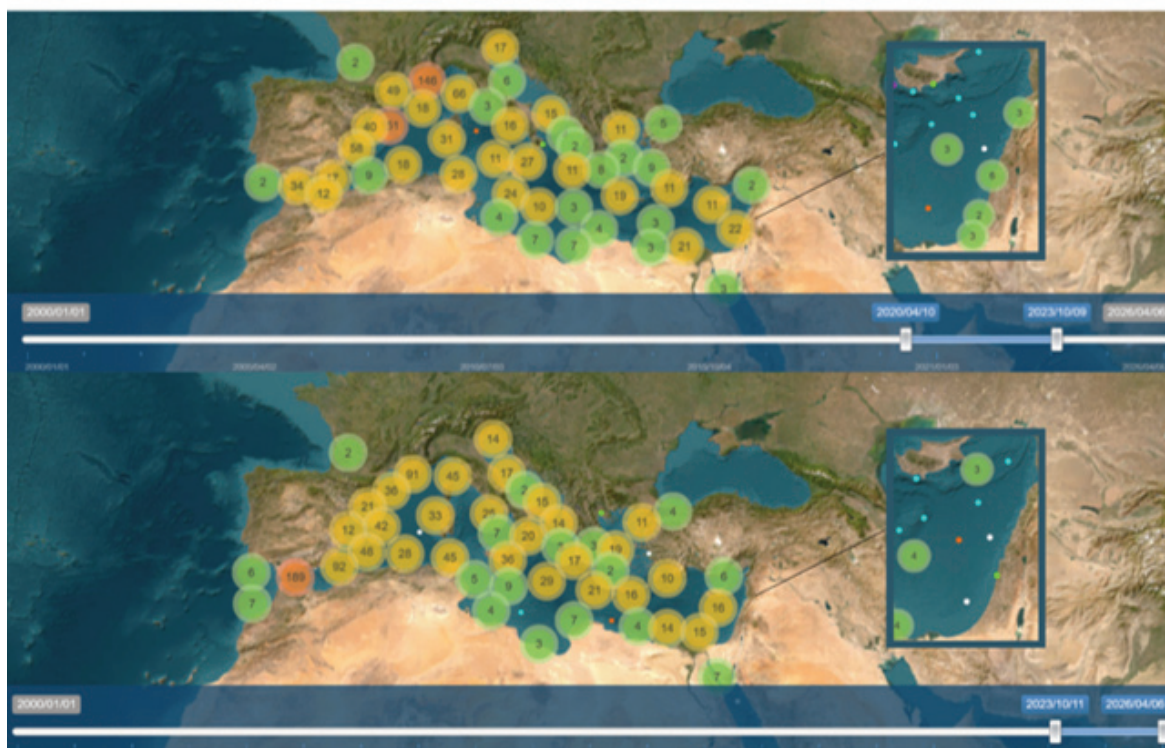
As central trade routes for essential goods like oil, chemicals, metal ores, and agricultural products, the Mediterranean and the Gulf remain vital areas for European economies. In 2023 alone, over two-thirds of all EU freight transported was by sea<sup>21</sup> (Eurostat, 2025). The shift in market shares of European fossil fuel suppliers following the Russian invasion of Ukraine underscores the Mediterranean's role as a vital corridor for diversified energy imports, and regional stability (Cong et al., 2024; Eurostat, 2025). With over 880,000 ship calls at EU ports in 2023, the sheer volume of traffic necessitates absolute situational awareness (European Maritime Safety Agency, 2025c). However, as maritime space becomes more contested, a dangerous trend emerges in which national authorities and private stakeholders increasingly opt out of transboundary data sharing. Fear of compromising critical infrastructure or revealing commercial vulnerabilities has created a fragmented data landscape with real costs. This becomes evident

<sup>21</sup> This statistic captures the total modal split performance in tonne-kilometers (tkm) across all transport modes within EU territory (maritime, road, rail, and inland waterways), including both international shipping and extensive intra-EU short-sea shipping routes. Measured strictly by raw weight (tonnes) or total financial value (€), land-based road transport dominates localised intra-EU cross-border trade, whereas maritime transport remains the dominant mode for long-distance, high-volume commodity corridors.

when looking at the number and distribution of data points shared through the MonGOOS Data Center. The maps

show that after 7 October, data sharing along the Levantine coastline was completely shut down (Figure 2).

**Figure 2.** Number and distribution of data points in the Mediterranean Oceanobs MonGOOS Data Center three years before and after 7 October 2023



Note. Sourced from oceanobs (2026).

The past Red Sea crisis illustrates this cost of uncertainty (Rai, 2025). Houthi attacks on merchant vessels since late 2023 have forced major carriers to reroute around the Cape of Good Hope, adding up to 4,000 miles and 10 days to Europe-Asia voyages, increasing transit times by roughly 30% and greenhouse gas emissions by 70% (Gallo, 2024; Szentivanyi, 2024; UNCTAD, 2024). This rerouting absorbed between 700,000 and 1.9 Million Twenty-Foot Equivalent Units of additional capacity, turning shippers into rate-takers in a market defined by scarcity (Arvis et al., 2026). In the concentrated freight industry, where the top four carriers provide 59% of global

liner capacity, integrated logistics determine global prices (Alphaliner, 2026). It is when these freight logistics hubs operate in data silos that the lack of reliable information becomes a systemic risk. Without real-time, shared insights on anomalies, whether they be pirate mother-vessels in the Gulf of Aden or hybrid threats in the Mediterranean, market players cannot optimise network effects, leading to massive inflationary pressures and supply chain fragility (Gallo, 2024; Kumar, 2026; Rai, 2025; Szentivanyi, 2024).

The paradox facing Mediterranean policy-makers is that the more a threat in-

Houthi attacks on merchant vessels since late 2023 have forced major carriers to reroute around the Cape of Good Hope, adding up to 4,000 miles and 10 days to Europe-Asia voyages, increasing transit times by roughly 30% and greenhouse gas emissions by 70%.

With its exceptional diversity, encompassing seven marine ecoregions and over 70 hydrological basins, this cooperation is required for effective governance of the Mediterranean Sea.

creases, as is currently evident with the 97% decline of shipping traffic in the Strait of Hormuz, the more protective states become over their operational data (Cao et al., 2026). If a coastal state hides its radar or environmental sensor data to protect national interests, it effectively prevents the early detection of transnational threats that could eventually paralyse its own ports. Hence, this approach to security-oriented withdrawal inadvertently decreases collective safety. Current trends towards proprietary data are not purely protective but incur real costs in freight rates, carbon emissions, and regional resilience (Rai, 2025). Conversely, European policy continues to demand more open-source, and Findable, Accessible, Interoperable, and Reusable (FAIR data and regulation (Ben Farah et al., 2022; Schaap et al., 2023). Importantly, not in all cases is the willingness of data holders the main challenge. Environmental monitoring and protection capacities vary across the Mediterranean, reflecting differences in institutional arrangements, technical resources, data management systems, and national priorities. These factors can affect the availability, comparability, and interoperability of environmental data, while marine pollution remains a persistent regional challenge (Interview with regional environmental governance expert; Copernicus, 2021).

### Transnational environmental interests in the Mediterranean

The recognition of interdependent common interests and transboundary environmental issues by different EU member states is exemplified by the UNEP/MAP framework conventions. The Barcelona Convention maintains a platform for regional dialogue and cooperation across changing political and geopolitical circumstances, demonstrating the potential for shared environ-

mental considerations to provide a basis for cooperation (Interview with regional environmental governance expert; Fry, 2025; Convention for the Protection of the Marine Environment and the Coastal Region of the Mediterranean, 1976). With its exceptional diversity, encompassing seven marine ecoregions and over 70 hydrological basins, this cooperation is required for effective governance of the Mediterranean Sea (Fry, 2025). Alongside the perspective of scarce resources leading to competition, there are many examples of cooperation over conflict. This is manifested by the Convention for the Protection of the Marine Environment and the Coastal Region of the Mediterranean (Barcelona Convention) and added Protocols, as well as the therein adopted Mediterranean Strategy for Sustainable Development (2016-2025) (UNEP/MAP, n.d.; Convention for the Protection of the Marine Environment and the Coastal Region of the Mediterranean, 1976; Mediterranean Strategy for Sustainable Development 2016-2025 - Investing in Environmental Sustainability to Achieve Social and Economic Development, 2016). In times of heightened geopolitical tensions, environmental cooperation may face additional challenges, as national security considerations often take precedence in governmental decision-making (Interview with regional environmental governance expert). Nonetheless, none of these agreements addresses the deprioritisation of environmental objectives during wars. This is partly because the absence of a military context in environmental policy ascribes to it a certain neutrality. So to protect “the Sea [that] is our life and our health” (Fry, 2025), environmental cooperation and its role must be appropriately framed within the securitised realities of the Mediterranean.

In the following, I present three cases that warrant information exchange for mutual

benefit in environmental cooperation: marine accidents, oil spills, and climate change. Firstly, localised stress signals are a bottleneck for decreasing accidents through policy intervention (Arvis et al., 2026). On average, an accident involving an EU member state-flagged ship occurs every 3 hours and 45 minutes (European Maritime Safety Agency, 2025c). Comparatively, at least one EU-flagged vessel suffers a very serious accident involving fatalities, total ship loss, or severe environmental damage every week (European Maritime Safety Agency, 2025c). To better prevent and respond to accidents, it is necessary to unlock partnerships between automatic identification system (AIS) data providers and regional organisations to produce real-time shipment visibility (Arvis et al., 2026). While increasing the agility of decision-making along maritime supply chains, unlocking cross-verified data would also help address latent accident risks from operating vessels built with outdated safety and damage stability standards (European Maritime Safety Agency, 2025c). As mentioned in the previous chapter, the European Maritime Safety Agency (EMSA) is one of the central actors for surveillance and early warning. Yet, its information services are more tailored to individual operators rather than cross-border crises.

Secondly, oil spills, with their devastating environmental and economic effects, are particularly common in the Eastern Mediterranean, where data sharing is scarcer. Strict environmental regulations, such as the MARPOL convention, have been put in place (REMPEC, 2022). It is vital for national and international authorities to have access to reliable, timely data, actively monitoring risks, spills, and potential polluters (Zakzouk et al., 2025). Synthetic Aperture Radar (SAR) imagery is only one example of such data, currently aiding the detection of oil discharge and spills. As illustrated in Figure 3, satellites measure the roughness

of the sea independent of weather conditions, making pollution visible. This helps with the forensics of oil spill detection. CleanSeaNet, the European oil spill monitoring and vessel detection service operated by EMSA since 2007, cross-checks SAR and optical data with other information, such as ship tracking data, to identify potential polluters (European Maritime Safety Agency, 2025b). EMSA then provides relevant authorities with valuable information to take further action. Under this service, a notification of a pollution event can be provided within 20 to 30 minutes of the satellite overpass (European Space Agency, 2007). Thereby, oil spill detection illustrates the merits of information exchange.

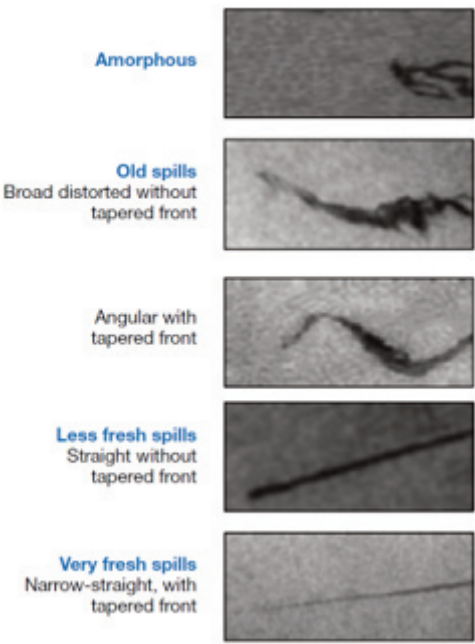
Thirdly, according to a MedECC report, a third of the Mediterranean population lives close to the Sea (MedECC, 2024). Events related to climate change, first and foremost rising sea levels, are anticipated to have devastating impacts on these areas, including the likely risk of flooding for at least three airports, 15 major ports, and numerous cultural world heritage sites identified by United Nations Educational, Scientific and Cultural Organization (UNESCO) in various countries (MedECC, 2024). The water quality of the sea is another issue of particular relevance for the EU and the Middle East and North Africa (MENA) region. Water quality not only affects ecosystems and industries, but also desalination projects and public health more broadly (Donderer & Lehrer, 2025). Heavily populated coastal areas, already subject to resource stress and rapid changes to the landscape like the Levantine coastline, are particularly affected (MedECC, 2020). Further contributing to poor water quality are mass tourism, population growth, new industries, and rapid urbanisation, as well as poor results in climate adaptation (Riccaboni et al., 2020). One example of such pollutants is offshore fish farms, as the organic load of excrements off the coast often exceeds

At least one EU-flagged vessel suffers a very serious accident involving fatalities, total ship loss, or severe environmental damage every week.

the ecosystem's processing capacity (Matijevic, 2021). An additional threat to the sustainability of maritime industries is current overfishing and aggressive methods leading to projections of 50% fishstock reduction by 2050 (MedECC, 2020; Riccaboni et al., 2020). This would not only affect coastal economies engaged in fishing, aquaculture, and related activities but would also increase the likelihood of quarrels over legitimate fishing rights among states, as already shown by multiple events in the Mediterra-

nean (FAO, 2020). With 32%, the Mediterranean Sea has the highest proportion of threatened marine habitats in Europe, with 21% being listed as vulnerable and 11% as endangered (MedECC, 2024). Sea populations are also likely to change as cold-water species move towards cooler waters and warm-water ones start to inhabit the Mediterranean, often with devastating consequences in the case of invasive species disturbing the ecosystem (Albano et al., 2021; MedECC, 2024).

**Figure 3.** Satellite imagery categorisation for remote oil spill detection



Note. Sourced from European Maritime Safety Agency (2025).

With 32%, the Mediterranean Sea has the highest proportion of threatened marine habitats in Europe, with 21% being listed as vulnerable and 11% as endangered.

Scholars have been warning for many years that warming waters, rising ocean acidification, and high pollutant loads are causing the collapse of native biodiversity along Levantine coastlines, intensifying and expanding geographically (Albano et al., 2021). Since all of these cycles are interconnected across borders, no single country could address these challenges alone (Fig-

ure 1) (Donderer & Lehrer, 2025). Adverse climate effects already disproportionately affect fragile countries, while resource extraction remains a dominant dynamic of conflict (Donderer & Lehrer, 2025; Fry, 2025). Digital innovation and routinely shared environmental data can aid alternate strategies for joint prosperity and stability in the Mediterranean region.

## An EU-Med Federated Learning architecture framework

Interconnected environments benefit from shared knowledge. Thus, data sharing emerged as a core function in environmental projects, such as the Blue Cloud 2026, with data exchange reaching peaks of 10 terabytes in a single month (Schaap et al., 2023). With the number of working sessions, averaging 2,870 per month and peaking at over 5,450, the scientific community's willingness for active engagement in environmental cooperation projects is evident (A Federated European FAIR and Open Research Ecosystem for Oceans, Seas, Coastal and Inland Waters, 2026; Schaap et al., 2023). Even though shared interests and cooperation across the Mediterranean prevail, so does a lack of transparency. States and private actors more commonly do not share data due to national security sensitivities or proprietary interests. Even so, while private data service providers such as Kpler or MarineTraffic provide baseline information, they function as centralised commercial brokers rather than neutral frameworks for building institutional trust in high-friction zones (Grigoropoulos et al., 2025). Within the wider European maritime security architecture, two primary decentralised models exist, though each operates under distinct structural constraints.

Within the EU, CISE functions as a voluntary data exchange framework connecting over 300 authorities (European Maritime Safety Agency, n.d.). For instance, it allows a Greek naval vessel, a Turkish coast guard, and a Maersk container ship to exchange information without a central commercial broker owning the conversation (European Maritime Safety Agency, 2022). By increasing data connectivity, including between military and civil institutions, one can harness synergies and avoid duplicate efforts (Euro-

pean Maritime Safety Agency, 2022). However, since CISE is designed fundamentally as an EU-internal semantic data-messaging framework, it faces complex legal and political hurdles when attempting to interface directly with non-EU littoral states in the Southern and Eastern Mediterranean. Even with EMSA's Integrated Maritime Services (IMS) or CleanSeaNet, data exchange remains largely ad-hoc and within public-authority networks (Zakzouk et al., 2025).

Beyond EU borders, the EU-funded the Critical Maritime Routes (CRIMARIO) initiative offers a vital blueprint for external cooperation through its Indo-Pacific Information Sharing (IORIS) platform (CRIMARIO, 2020). Developed specifically for non-EU partner states and provided free of charge, IORIS is a neutral, secure operational coordination tool utilised by over 150 agencies across 50 countries to manage transboundary threats, including maritime pollution, search-and-rescue, and illegal, unreported, and unregulated fishing (Service for Foreign Policy Instruments, 2025). The IORIS platform demonstrates that regional neighbours are highly receptive to environmental and safety metrics as politically neutral entry points for maritime diplomacy, provided they maintain strict autonomy over their data streams (IORIS, 2025). Yet, despite the success of IORIS's community model, its reliance on the active, voluntary transmission of operational data and formatted reports across a web-based network may be a participation barrier in times of conflict.

Therefore, the next generation of EU-funded Mediterranean information environments should synthesise the decentralised messaging philosophy of CISE with the external partner-facing mandate of IORIS, advancing the architecture into a privacy-preserving Federated Learning (FL) AI framework. By implementing an FL-driven Blue Data Bridge, the EU can shift from voluntary

The IORIS platform demonstrates that regional neighbours are highly receptive to environmental and safety metrics as politically neutral entry points for maritime diplomacy, provided they maintain strict autonomy over their data streams.

Despite the recognised potential of AI for environmental monitoring, the majority of current AI projects do not address issues on Sustainable Development Goal (SDG).

data transmission to automated, edge-computed interoperability. By providing a secure plug-and-play environment fusing insights from commercial data with national sensor data, the Blue Data Bridge would increase collective knowledge and shared situational awareness (Schaap et al., 2023).

FL AI models allow for data insights without direct exchange, ensuring proprietary and protected information never leaves the owner’s server (Bhanbhro et al., 2024). Within the FL architecture, different actors collaboratively train a model while keeping the data on local servers. For instance, a shipping company or a navy can train a shared AI model for anomaly detection on their own local servers. This means that clients only share model updates with the central server (Bhanbhro et al., 2024; Graser et al., 2024). By design, the central system aggregates the mathematical model weights, the algorithmic learning, rather than the raw data itself, protecting sensitive inputs like exact coordinates, commercial cargoes, or patrol routes. While advanced differential privacy guards are required to prevent adversarial reverse-engineering of these model weights, raw data remains behind firewalls. The FL server then aggregates the model updates into the global model and returns

the global model to the clients for further training (Interview with Graser).

There lies an untapped opportunity in applying AI innovation to the maritime domain. Notably, despite the recognised potential of AI for environmental monitoring, the majority of current AI projects do not address issues on Sustainable Development Goal (SDG) 6, Clean water and sanitation, SDG 14, Life below water, nor SDG 16, Peace, justice, and strong institutions (Cowls et al., 2021). Additionally, current EU-Horizon projects either tend to focus their Federated Learning applications on the realms of transportation and medical applications, or take place in the Baltic Sea, except for the Blue Cloud 2026 project in the Mediterranean (A Federated European FAIR and Open Research Ecosystem for Oceans, Seas, Coastal and Inland Waters, 2026; European Commission, n.d.-b; Graser et al., 2025). This project does not use AI but draws attention to the vast information already present in the Mediterranean maritime context (Table 1). An FL model could tap into existing resources of EMSA, including CleanSeaNet, as a baseline for learning, and gradually incorporate more unconventional data sources from local nodes (Table 1).

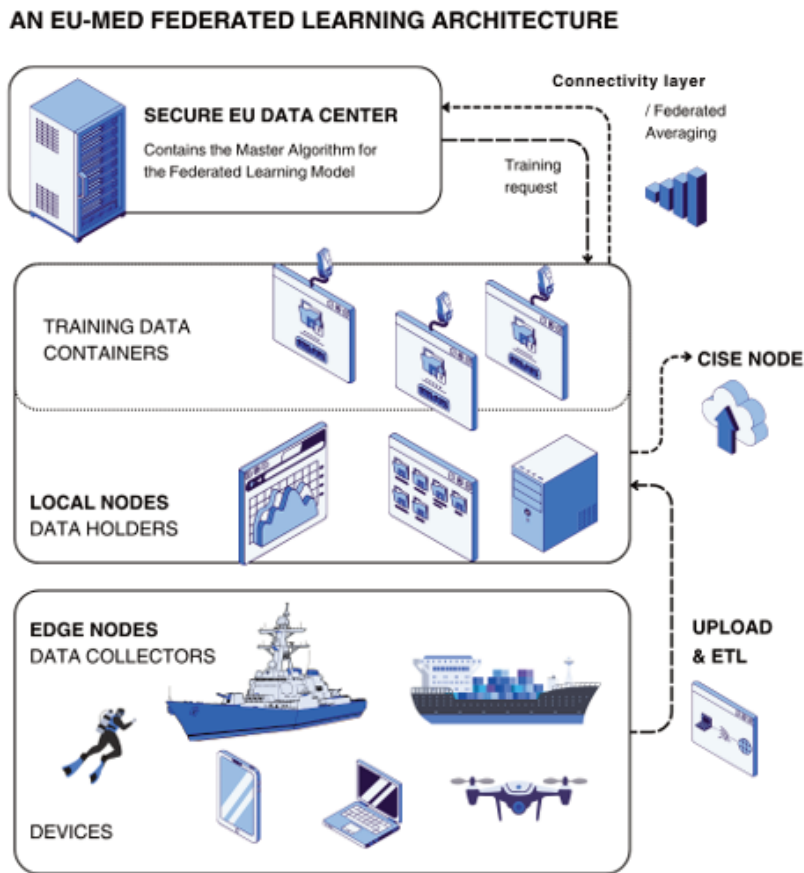
Table 1. Existing data architecture of the EU-Med and relevance for Federated Learning

| Data-Architecture Type     | Definition                                                        | EU Systems                                                                                                       | Role for Federated Learning                                                                                   |
|----------------------------|-------------------------------------------------------------------|------------------------------------------------------------------------------------------------------------------|---------------------------------------------------------------------------------------------------------------|
| Central Hubs (Aggregators) | Data is collected and processed at one physical location          | Copernicus Marine, MarineTraffic / Kpler AIS, CleanSeaNet (EMSA), SafeSeaNet, Central Ship Database (CSD), SOCAT | The Global Model: This is where the master algorithm is trained, as large, harmonized datasets are available  |
| Federated Networks         | Data remains with local nodes, but can be accessed via interfaces | CISE, IORIS, Blue-Cloud 2026, SeaDataNet, EMODnet, MonGOOS, DITTO (Digital Twin Ocean)                           | The FL Framework: These systems provide the infrastructure (APIs/protocols) to send the algorithm to the data |

|                                |                                                                                        |                                                                              |                                                                                                                |
|--------------------------------|----------------------------------------------------------------------------------------|------------------------------------------------------------------------------|----------------------------------------------------------------------------------------------------------------|
| <b>Local Nodes (Edge-Data)</b> | Primary data source located directly on-site. Often sensitive or too large to transfer | Coastal Radar, VMS data from fisheries, CS-MACH1, Euro-Argo, SIOS, JERICO-RI | The Training Nodes: Where local learning takes place. The raw radar images or sensor data never leave the node |
| <b>Innovation-Drivers</b>      | New initiatives that expand the technological horizon or frame the use case            | OceanEye (EU 2026), World Database on Protected Areas (MPAs)                 | The Use-Case: Defining the areas (e.g., MPAs) in which the FL models are applied with priority                 |

Note. Elaborated by author, sourced from A Federated European FAIR and Open Research Ecosystem for Oceans, Seas, Coastal and Inland Waters (2026); European Maritime Safety Agency (2022, 2025b, 2025a); Grigoropoulos et al. (2025); Kapidani et al. (2022); Mercator Ocean International (2025); oceanobs (n.d.); Schaap et al. (2023); and Vasileva & Ahmed (2020).

Figure 4. Model framework of an EU-Med Federated learning architecture



Note. Elaborated by author.

Based on the existing data architecture of the EU-Med, I present a potential architecture for a European Maritime Federated AI. The model has three levels with different Extract, Transform, and Load (ETL) processes in between (Figure 4).

▪ **Edge Nodes (Data collectors and devices):**

The first step in building regional situational awareness and learning is local data collection. This can be done by diverse actors, including but not limited to dive centres, sailors, universities, schools, naval authorities, and private shipping companies. These actors use devices such as GPS, drones, sensors, apps, and others to collect different data types. These may include encrypted position reports from patrolling vessels, position reports from leisure crafts, photographs from dive sites, or additional meteorological-oceanographic data provided by buoys.

- **Upload and ETL:** In the first step, data holders must extract relevant features for analysis from their collected data. Sensitive metadata, such as the specific identity of a private leisure craft or naval officer, is removed or coded to ensure compliance with GDPR and national security protocols. Second, data ideally follows principles of FAIRness and if necessary<sup>22</sup>, is converted into standardised formats, such as those by EMODnet or Sea-DataNet (Interview with Dr. Jaume Piera Fernández, Tenured Scientist at the Institute of Marine Sciences [ICM-CSIC]). Most critical is creating context for the information. For instance, divers label a photograph of a Posidonia meadow and tag it with its GPS location, size measurements, and turbidity context. Lastly, the cleaned, anonymised, and formatted

data is loaded into a local training container on the actor's server. This container is a restricted environment where the EU's FL model can operate without ever accessing the rest of the organisation's private database. To maintain the data privacy granted by FL solutions, the ETL process occurs entirely within the local jurisdiction of the data collector.

▪ **Local Nodes (Data holders, and training data containers):**

The data holders can be naval authorities, private companies, such as CMA CGM, public authorities, such as EMSA, non-governmental institutions, like Acarbio, or universities, such as the Interuniversity Institute of Marine Science, to name a few (see Table 1). These actors would prepare and store relevant data for AI training on their local servers. An EU authority will supply the Federated Learning model(s) for specific use cases, which are sent to local nodes in real time, periodically, or upon training requests.

- **Node:** Besides the Federated Learning model exchange, local data holders may provide their raw data to other actors within the system architecture upon request. As with CISE, the system then facilitates the communication and interoperability for data exchange between local nodes. Conversely, CISE and IORIS members can use insights from the FL model to identify the exact information requests that truly require a manual raw-data request. This saves bandwidth and increases data sovereignty.

▪ **Secure EU Data Centre:** The master algorithm of the FL model itself resides on a secure EMSA data server (struc-

<sup>22</sup> In the case of AIS data, further standardisation is not necessary.

ture). When the model is sent to local servers for training, it compares new, previously unknown data records to the existing model. Examining the deviation between record and model helps, for instance, in giving a reason for vessel movement or sea surface temperature anomalies. Most critical for the structural longevity of such an architecture is that ownership of the Data Centre is not dependent on private organisations or proprietary software.

- **Connectivity layer for model updates:** The core of FL solutions is their connectivity layer. Herein, model updates from local nodes are aggregated and combined. There are many ways to combine updates for incorporation into the global model, a common one being federated averaging, which, as the name implies, calculates the weighted average of all updates. Since data quality will vary across local nodes, the method chosen should account for data quality scores in its weighing. A considerable advantage of the connectivity layer is that it generates insights without massive computational resources. It also allows FL solutions to compensate for local information not being available for periods of time (Interview with Graser). The technical environment for this step could be gRPC, a modern open-source high-performance Remote Procedure Call (RPC) framework that can connect services in and across data centres and run in any environment (GRPC, 2026). gRPC enables asynchronous learning, ideal for information resilience in the maritime context, where vessels may be offline for days and can only connect to the model when they have satellite or port connectivity.

In the first phase, a FL model for a specific use case could be primarily designed for

EU member states and provided as AI-as-a-Service. A promising case study could be a model trained on vessel pattern recognition, predicting where vessels show anomalies in movement, specifically to detect piracy or dragging patterns near critical infrastructure such as subsea cables, without requiring nations to share their raw patrol routes. A good practice example is the FL model developed by Gräupl and colleagues in 2025, which draws a pathway for improving data privacy while simultaneously reducing communication costs in machine learning for movement anomaly detection. Notably, their maritime movement anomaly detection model reduced communication bandwidth requirements by approximately 86-98%, enabling anomaly model training in low-and/or expensive-bandwidth regions such as the Sea (Gräupl et al., 2025). However, in the context of ongoing wars, an EU-funded FL on subsea cables and vessel movement may trigger security concerns in neighbouring countries and hamper engagement beyond the first phase (Interview with Dr. Viviana Piermattei, a Scientist in Oceanographic Observations and Technologies Development at CMCC Foundation). A more incremental approach to leverage FL models for a shared Maritime Ground Truth layer is recommended, in which environmental monitoring is regarded as the primary entry point for diplomatic exchange (Interview with Doug Weir, Director of Conflict and Environment Observatory; Idibekzoda, 2024; Moussaoui & Rachid, 2023). In this regard, Dr. Piera Fernández points out that biodiversity data will be a lucrative business in the future. Despite existing digital tools for biodiversity data collection like iNaturalist, there is little shared environmental intelligence on the root causes, processes, and effects of changes observed in the data, as well as their dependence on physical parameters. An FL solution in this context could not only address the

In the context of ongoing wars, an EU-funded FL on subsea cables and vessel movement may trigger security concerns in neighbouring countries and hamper engagement beyond the first phase.

above-mentioned concerns regarding proprietary software and data, but also help in closing this significant knowledge gap with verified truths.

To keep up momentum, the second phase of the EU-Med FL architecture must focus on stakeholder engagement and capacity building. Innovation in data annotation and analysis can be driven by integrating automated processes with human oversight, transforming data collection into a dynamic, participatory ecosystem. For one, many Mediterranean datasets at scale make manual data cleaning by local data holders infeasible. The CrowdSeaMapping project addressed this by deploying onboard AI models, flagging measurements that deviate significantly from learned distributions locally, thereby easing barriers for contributing local authorities (Graser et al., 2025). To further increase the reliability of the FL model, interviewees recommend integrating AI-based information with human verification (Catalli et al., 2026). In this so-called human-in-the-loop workflow, domain experts and hydrographers can act as data annotators or verifiers, assessing data context or flagged model updates to determine if they are valid environmental deviations or mere outliers (Catalli et al., 2026; Interview with Piera Fernández). This creates a continuous cross-validation in which expert intervention refines the machine learning model's accuracy while simultaneously updating the underlying data references. This collaborative approach enhances the accountability and trust necessary for AI applications in sensitive maritime corridors (Catalli et al., 2026). Yet, not just experts can become active contributors to the model. Dr. Piermattei points out that with the emergence of no- and low-code systems, as well as the rising programming literacy in youth, student involvement in model calibration after deployment of low-cost sensors and data collection would build long-lasting capacity

while aiding continued innovation. The adoption of the model beyond EU borders can be gradually opened to Mediterranean partners who express interest, similar to the roll-out of CRIMARIO, an EU initiative for the safety of Indo-Pacific maritime routes.

### Desecuritising regional relations through federated learning

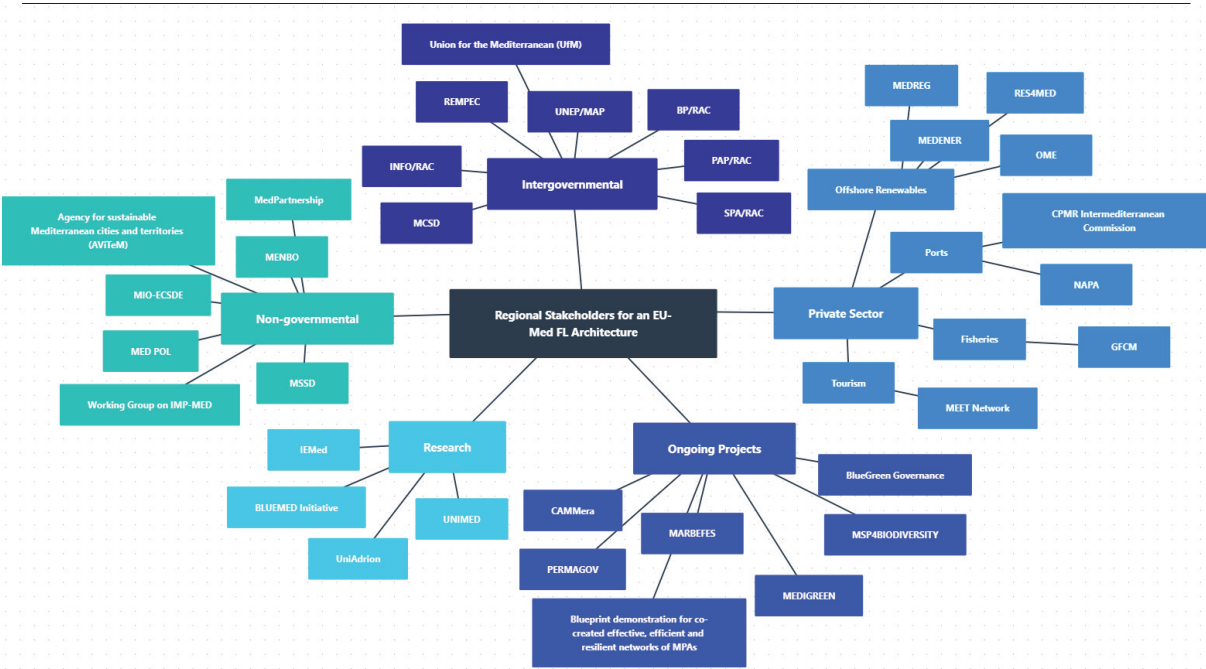
The Blue Data Bridge can create somewhat stable, predictable, and routinised relations of regional situational awareness and shared analysis between actors. The proposed model opens horizons for actors from adversarial states, such as Türkiye, Cyprus, Lebanon, and Israel-Palestine, to cooperate without the political cost of formal recognition or boundary concessions. This transforms points of contestation into shared environmental zones, using technical data as the primary diplomatic currency (Hogg et al., 2024; Moussaoui & Rachid, 2023). Hence, FL approaches provide a technical and political roadmap for maritime data sharing that addresses the trust versus transparency dilemma. In times of budget cuts and austerity measures, this allows EU member states to use the same technology and the same resources to work on different problems. Thus, the EU should continue this integration with an increased use of satellites, and further examine if it is already taking full advantage of new technology that makes it easier to prevent and govern shared risks. Arguably, when regional neighbors and non-state actors operate from a shared Common Operational Picture (COP), they are more resilient to shocks from attacks alike those of the Houthis. This is because they can act on the same real-time data to coordinate alternative shipping routes, predict attack patterns, and ensure that one actor does not paralyse the entire supply chain (Mihailovic et al., 2022). It

In this so-called human-in-the-loop workflow, domain experts and hydrographers can act as data annotators or verifiers, assessing data context or flagged model updates to determine if they are valid environmental deviations or mere outliers.

may be inferred that this improved network resilience would lower the rate of shipping performance decline after attacks (Cong et al., 2024). The Blue Data Bridge is one strategy to strengthen regional stability rather than competing national security in-

terests by challenging the increasing militarisation of maritime spaces and turning data insights into a public good for sustainable development, disaster risk reduction, search-and-rescue, and many more critical interventions.

**Figure 5.** Network Map of relevant regional stakeholders for the implementation of an EU-Med Federated Learning architecture



Note. Elaborated by author.

Nonetheless, the potential success of an EU-Med FL model relies on its governance (Interview with regional environmental governance expert). Figure 5 illustrates only some of the currently relevant regional stakeholders that must be considered for implementation. Because participants of the FL do not view each other's raw data, verifying the quality and truthfulness of local data inputs becomes difficult. Poor local data collection or intentional data-poisoning by a participant will also degrade the global model. IORIS provides invaluable operational lessons on handling low-trust or adversarial participants in contested waters by establishing so-called

«Communities of Choice», which are user-defined, encrypted sub-groups that allow states to isolate information exchange to specific partners or functional missions without exposing data to regional competitors. Additionally, any future EU-Med FL must integrate automated and participatory data-validation protocols before weights are accepted. To protect participants from fatigue, they should not only co-create data but also co-benefit from model results. For instance, in biodiversity monitoring, FL insights can help guide procedures, protocols, and training materials so they become more accessible and relevant (Interview with Dr. Maria

Any future EU-Med FL must integrate automated and participatory data-validation protocols before weights are accepted.

Ojanen, Senior Research Scientist at the Finnish Environment Institute). For this, the differing interests of stakeholders must be taken into account. In the case of conservation, not all stakeholders who are relevant data holders share the premise of protecting ecosystems (Interview with Ojanen). These must be otherwise incentivised (Interview with Piera Fernández). Moreover, should interventions and decisions be derived from the EU-Med FL, assigning liability becomes central. The European External Action Service (EEAS) and the Union for the Mediterranean (UfM) must establish a clear legal charter defining whether liability rests with the node that generated an alert, the central aggregator, or the operational authority executing any response.

## Conclusion and policy recommendations

This chapter advocates for an EU-hosted Mediterranean Open-Access Ground

Truth layer – the Blue Data Bridge. To move from friction to stability, we must treat maritime data as a shared environmental resource. It is timely for regional policy to evolve from limited data exchange to active, intelligent layers (European Maritime Safety Agency, 2022). By using FL, a decentralised AI approach, states, private actors, and non-governmental organizations (NGOs) can train environmental algorithms on their own data, sharing only insights instead of raw data (Bhanbhro et al., 2024). This creates a Blue Data Bridge that supports both the European Ocean Pact (2025) and the Water Resilience Strategy, while building trust between potentially hostile parties (European Water Resilience Strategy, 2025; The European Ocean Pact, 2025). FL enables privacy-preserving data analy-

sis, providing states with more predictable information and routinised, secure exchange with other actors, effectively demopolising situational awareness (Donderer 2021; Mitzen 2006). This forces a shift from hiding data to verifying data, lowering the risk of miscalculation based on false information. In regions like the Gulf of Aqaba or the Aegean, where neighbouring states are in deadlock, the proposed FL architecture can provide triangulated information on vessel routes, disaster risks, and environmental monitoring, effectively de-securitising surveillance by making information a public good.

EMSA appears to be the critical actor for deploying a FL architecture. Therein, aggregating environmental monitoring data from both private providers, such as Kpler, and public sensors, such as those from CleanSeaNet, without exposing the underlying source sensitivity (Zakzouk et al., 2025). This would allow more public and private actors to operate from a shared COP, have access to valuable insights for Track II diplomacy, and create more routinised, stable relations in increasingly militarised contexts (Fry, 2025; Mitzen, 2006). As is customary for CISE and IORIS, information exchange would be voluntary rather than mandated by legislation. Nevertheless, different incentive structures can help attract engagement across different sectors. Academic stakeholders show a high willingness to adopt an FL-model for environmental monitoring in the Mediterranean (Interview with Ojanen, Piera Fernández, and Piermattei). Besides an intrinsic motivation for more complete information, interviewees note that the FL approach could help address the common hurdle of data verification in current monitoring and detection efforts (Interview with Piermattei and Ojanen). As opposed to public and research institutions, the private sector relies more

strongly on policy and financial incentives to engage in innovation measures alike FL (Interview with Graser). EU-backed insurance guarantees or expedited port clearance were mentioned as potential motivations for companies to engage in FL (Interview with Graser, and Piermattei). Data trustees could act as intermediaries, simplifying access to sensitive data and ensuring its long-term use for science and society (Interview with Piera Fernández). In addition to obligations, incentives such as tax breaks for data donations and intangible accounting options for companies should be created (Kapidani et al., 2022). Further incentives could include restricting access to specific functions to data providers or increasing their visibility on data portals to actively promote the exchange and use of environmental data (Catalli et al., 2026).

Based on the findings, the following recommendations are given to policymakers:

1. **The European Commission (Directorate-General for Maritime Affairs and Fisheries [DG MARE]), in coordination EMSA, must prioritise developing a Mediterranean FL pilot architecture** using open-source frameworks and public server structures, specifically targeting a transboundary use case like the SafeSeaNet and Marine Protect Area (MPA) intersection. Such architecture helps leverage existing information through advanced stakeholder interaction and federated deep learning, ensuring sensitive data remains strictly under national sovereignty. This strengthens EU strategic autonomy at sea by reducing reliance on United States (US)-owned server structures in Europe. Investing in decentralised data infrastructure becomes even more pertinent in light of information security and the dramatic proliferation of cybercrimes fuelled by
- increased levels of technological systems integration (Ben Farah et al., 2022). The proposal aligns with the EU Data Strategy's goal of creating sovereign data spaces where governance of the master algorithm is placed under a joint oversight body such as a dedicated committee within the UfM.
2. **EEAS and UfM should explicitly link environmental monitoring, such as ICZM Protocol compliance, with regional maritime security protocols** in future policy updates. This step helps shift the perception of data sharing from a security risk to a security asset. By positioning environmental health as a prerequisite for regional prosperity and maritime stability, states are incentivised to pursue shared transboundary interests. To underpin this initiative, the Council of the European Union should mandate Maritime Environmental Health as a non-sensitive shared data category within the biennial EUMSS Progress Reports. This aligns with the 2023 EUMSS Update, which identifies environmental degradation as a direct threat to maritime security.
3. **Horizon Europe, the European Climate, Infrastructure and Environment Executive Agency (CINEA), and the Mediterranean Action Plan (UNEP/MAP) should allocate funding for the second phase of stakeholder engagement.** This phase focuses on hybrid recognition models that integrate expert hydrographers and citizen scientists into automated ETL pipelines. This ensures the structural longevity of the Blue Data Bridge and supports the European Research Area (ERA) goals by lowering barriers for youth and students and ensuring that AI remains accountable and trusted. A collaboration with the Co-

pernicus Marine Service National Collaboration Programme (NCP) may be envisioned to boost user engagement (Copernicus, n.d.).

4. **EU Member State Transport Ministries and the European Ports Association must be involved to devise and implement policy incentives**, such as port clearance priority or reduced taxes for private carriers that integrate their local data into the FL training nodes. By providing incentives for participation in the model, the EU can leverage the market power of major logistics hubs to feed regional insights without compromising the industry's commercial independence.
5. **The European Commission, supported by regional research net-**

**works like the European Institute of the Mediterranean (IEMed), is encouraged to establish a permanent, cross-sectoral Blue Data Bridge Dialogue Forum** to translate Federated AI insights into real-time maritime policy and adjustments. The Forum provides a backdoor for Track II diplomacy between marine civil society and private sector actors, such as Marine Insurance Consortia in the Levant and Northern Africa. The Forum will act as a living community championing joint situational awareness and closing the feedback loop between technology and governance. Thereby, it supports the Dynamic Marine Spatial Planning required for the success of the Marine Strategy Framework Directive (MSFD) and Barcelona Convention.

## References

- ALBANO, P. G., STEGEN, J., BOŠNJAK, M., DUNNE, B., GUIFARRO, Z., TURAPOVA, E., HUA, Q., KAUFMANN, D. S., RILOV, G., & ZUSCHIN, M. (2021). Native biodiversity collapse in the eastern Mediterranean. *Proceedings. Biological Sciences / the Royal Society*, 288(1942), 1-9. <https://doi.org/10.1098/rspb.2020.2469>
- ARVIS, J.-F., RODRIGUE, J.-P., ULYBINA, D., & RASTOGI, C. (2026). A metric of global maritime supply chain disruptions: The global supply chain stress index - maritime (GSCSI-M). *Journal of Transport Geography*, 131, 1-14. <https://doi.org/10.1016/j.jtrangeo.2026.104575>
- ARVIS, J.-F., VESIN, V., CARRUTHERS, R., DUCRUET, C., & DE LANGEN, P. (2019). *Maritime networks, port efficiency, and hinterland connectivity in the mediterranean*. World Bank Group. <https://openknowledge.worldbank.org/entities/publication/f75ac835-6ab9-5a76-8110-86065ad8bc65>
- BEN FARAH, M. A., UKWANDU, E., HINDY, H., BROSSET, D., BURES, M., ANDONOVIC, I., & BELLEKENS, X. (2022). Cyber security in the maritime industry: A systematic survey of recent advances and future trends. *Information*, 13(1), 22, 1-33. <https://doi.org/10.3390/info13010022>
- BERMAN, N. (2024). *How Houthi Attacks in the Red Sea Threaten Global Shipping*. Council on Foreign Relations. <https://www.cfr.org/articles/how-houthi-attacks-red-sea-threaten-global-shipping>
- BHANBHRO, J., NISTICÒ, S., & PALOPOLI, L. (2024). Issues in federated learning: some experiments and preliminary results. *Scientific Reports*, 14(1), 29881, 1-15. <https://doi.org/10.1038/s41598-024-81732-0>
- BOUSTROS, E. (2018). *Natural Gas in East-Mediterranean Basin – Changing the Energy Landscape*. [https://www.researchgate.net/publication/329453610\\_Natural\\_Gas\\_in\\_East-Mediterranean\\_Basin\\_-\\_Changing\\_the\\_Energy\\_Landscape](https://www.researchgate.net/publication/329453610_Natural_Gas_in_East-Mediterranean_Basin_-_Changing_the_Energy_Landscape)
- CAO, Y., WANG, H., SU, F., FU, D., YAN, F., HONG, X., HE, W., XU, N., OU, Y., & CHEN, C. (2026). Satellite radar and AIS reveal a 97% decline in shipping traffic through the Strait of Hormuz. *The Innovation*, 7(6), 101367, 1-3. <https://doi.org/10.1016/j.xinn.2026.101367>
- CATALLI, F., HOCHNEGGER, F., REITZ, T., KLIEN, E., KOCON, K., & KRÄMER, M. (2026). *Nachhaltigkeitspotentialanalyse für die Zweckmäßigkeit und den Aufwand von Datenannotationen für Machine Learning (ML)-Modelle*. German Environment Agency. [https://www.umweltbundesamt.de/system/files/medien/11850/publikationen/2026-03/25\\_2026\\_TEXTE.pdf](https://www.umweltbundesamt.de/system/files/medien/11850/publikationen/2026-03/25_2026_TEXTE.pdf)

- CONG, L., ZHANG, H., WANG, P., CHU, C., & WANG, J. (2024). Impact of the Russia–Ukraine Conflict on Global Marine Network Based on Massive Vessel Trajectories. *Remote Sensing*, 16(8), 1329, 1-20. <https://www.mdpi.com/2072-4292/16/8/1329>
- COPERNICUS MARINE SERVICE. (n.d.). *National Collaboration Programme. Copernicus Marine Service*. Retrieved April 10 2026 from <https://marine.copernicus.eu/services/national-collaboration-programme>
- COPERNICUS MARINE SERVICE. (2021). *OBSERVER: Tracking oil spills with Copernicus*. Copernicus Maritime Service. <https://www.copernicus.eu/en/news/news/observer-tracking-oil-spills-copernicus>
- COUNCIL OF THE EUROPEAN UNION. (2014). *European Union Maritime Security Strategy, Pub. L. No. 11205/14*. Council of the European Union. <https://data.consilium.europa.eu/doc/document/ST%2011205%202014%20INIT/EN/pdf>
- COWLS, J., TSAMADOS, A., TADDEO, M., & FLORIDI, L. (2021). A definition, benchmark, and database of AI for social good initiatives. *Nature Machine Intelligence*, 3(2), 111–115. <https://doi.org/10.1038/s42256-021-00296-0>
- CRAMER, W., GUIOT, J., & MARINI, K. (Eds.). (2020). *Climate and Environmental Change in the Mediterranean Basin – Current Situation and Risks for the Future. First Mediterranean Assessment Report*. Union for the Mediterranean, Plan Bleu, UNEP/MAP, MedECC. <https://www.medecc.org/mececc-reports/climate-and-environmental-change-in-the-mediterranean-basin-current-situation-and-risks-for-the-future-1st-mediterranean-assessment-report/>
- DJOUNDOURIAN, S., LIONELLO, M., LLASAT, C., GUIOT, J., CRAMER, W., DRIQUECH, F., GATTACCECA, J. C., & MARINI, K (Eds.). (2024). *Special Report on Climate and Environmental Coastal Risks in the Mediterranean*. MedECC. <https://www.medecc.org/mececc-reports/med-coastal-risks/>
- DI PERI, R., & MEIER, D. (2023). *Mediterranean in dis/order: space, power, and identity*. University of Michigan Press. <https://doi.org/10.3998/mpub.12307776>
- DONDERER E., & LEHRER, D. (2025). *Shared Environments, Shared Futures*. Arava Institute for Environmental Studies. <https://arava.org/wp-content/uploads/2025/09/Shared-Environments-Shared-Futures-September-2025-report.pdf>
- DONDERER, E. (2021). *Ontological Insecurity: A Case Study on Israeli-Palestinian Conflict in Jerusalem*. E-International Relations. <https://www.e-ir.info/2021/07/23/ontological-insecurity-a-case-study-on-israeli-palestinian-conflict-in-jerusalem/>
- EHTESHAMI, A., & MOHAMMADI, A. (2017). *The Key Powers' Construction of the Mediterranean*. Barcelona Centre for International Affairs. <https://www.cidob.org/en/publications/key-powers-construction-mediterranean>

EUROPEAN COMMISSION. (2026). *A federated European FAIR and Open Research Ecosystem for oceans, seas, coastal and inland waters*. European Commission, Horizon Europe. <https://cordis.europa.eu/project/id/101094227>

EUROPEAN COMMISSION. (n.d.-a). *East Mediterranean: General introduction to the Eastern Mediterranean Sea basin. European MSP Platform*. European Commission, European MSP Platform. Retrieved April 10 2026 from <https://maritime-spatial-planning.ec.europa.eu/sea-basins/east-mediterranean>

EUROPEAN COMMISSION. (n.d.-b). *Search “federated” “learning” “med.” CORDIS - EU Research Results*. European Commission, CORDIS. Retrieved April 10 2026 from [https://cordis.europa.eu/search?q=contenttype%3D%27project%27%20AND%20frameworkProgramme%3D%27HORIZON%27%20AND%20\(%27federated%27%20AND%20%27learning%27%20AND%20%27med%27\)&p=1&num=10&sort=Relevance:decreasing](https://cordis.europa.eu/search?q=contenttype%3D%27project%27%20AND%20frameworkProgramme%3D%27HORIZON%27%20AND%20(%27federated%27%20AND%20%27learning%27%20AND%20%27med%27)&p=1&num=10&sort=Relevance:decreasing)

EUROPEAN SPACE AGENCY (ESA). (2007). *EC unveils new EU maritime policy*. ESA. Retrieved April 06 2026 from [https://www.esa.int/Applications/Observing\\_the\\_Earth/EC\\_unveils\\_new\\_EU\\_maritime\\_policy](https://www.esa.int/Applications/Observing_the_Earth/EC_unveils_new_EU_maritime_policy)

EUROPEAN COMMISSION. (2023). *Blue-Cloud 2026: A federated European FAIR and Open Research Ecosystem for oceans, seas, coastal and inland waters [Data management plan]*. European Union’s Horizon Europe research and innovation programme. <https://cordis.europa.eu/project/id/101094227>

EUROPEAN COMMISSION. (2025). *European Water Resilience Strategy, Pub. L. No. COM(2025) 280, 52025DC0280*. European Commission. [https://environment.ec.europa.eu/publications/european-water-resilience-strategy\\_en](https://environment.ec.europa.eu/publications/european-water-resilience-strategy_en)

EUROPEAN COMMISSION (2025). *The European Ocean Pact, Pub. L. No. COM/2025/281, 52025DC0281*. European Commission.

EUROPEAN MARITIME SECURITY AGENCY. (n.d.). *Common Information Sharing Environment (CISE) - Operational Phase*. European Maritime Security Agency. Retrieved April 8 2026 from <https://emsa.europa.eu/cise/operational-phase.html>

EUROPEAN MARITIME SECURITY AGENCY. (2022). *CISE Architecture (2nd ed.)*. European Maritime Safety Agency.

EUROPEAN MARITIME SECURITY AGENCY. (2025a). *Enhanced maritime picture via Integrated Maritime Services - Data sources*. European Maritime Security Agency. <https://emsa.europa.eu/combined-maritime-data-menu/data-sources.html>

EUROPEAN MARITIME SECURITY AGENCY. (2025b). *Maritime Digital Services Catalogue 2025*. European Maritime Safety Agency.

<https://www.emsa.europa.eu/we-do/digitalisation/77-publications/4449-maritime-digital-services-catalogue.html>

EUROPEAN MARITIME SECURITY AGENCY. (2025c). *The 2025 European Maritime Safety Report*. European Maritime Security Agency. <https://www.emsa.europa.eu/publications/item/5598-emsafe-report-2025.html>

EUROSTAT. (2025). *Most goods transported by sea within the EU in 2023*. Eurostat. <https://ec.europa.eu/eurostat/web/products-eurostat-news/w/ddn-20250416-1>

FLANDERS MARINE INSTITUTE. (2023). *Maritime boundaries geodatabase* (Version 12) [Data set]. <https://doi.org/10.14284/628>

FRY, D. P. (2025). Peace and sustainability through partnership and cooperation: Generalizable lessons from Norden and the Mediterranean. *Peace and Sustainability*, 1(1), 100003, 1–9. <https://doi.org/10.1016/j.nerpsj.2025.100003>

GALLO, A. (2024). The mediterranean maritime network of container shipping: spatial structure and regional dynamics. In O. Gervasi, B. Murgante, C. Garau, D. Taniar, A. M. A. C. Rocha, & M. N. Faginas Lago (Eds.), *Computational science and its applications – ICCSA 2024 workshops: hanoi, vietnam, july 1–4, 2024, proceedings, part X* (Vol. 14824, pp. 300–314). Springer Nature Switzerland. [https://doi.org/10.1007/978-3-031-65332-2\\_20](https://doi.org/10.1007/978-3-031-65332-2_20)

GERMOND, B. (2015). *The maritime dimension of european security: seapower and the european union*. Palgrave Macmillan UK. <https://doi.org/10.1057/9781137017819>

GRASER, A., NIELSEN, N. B., & ANDERSEN, O. (2025). *Crowdsourced Seafloor Mapping: Federated Learning at the Edge*. Geodatastyrelsen. <https://gst.dk/ansvar-somraader/soekort-og-marine-data/eksternt-finansierede-projekter/mobispaces/blog-post-crowdsourced-seafloor-mapping-federated-learning-at-the-edge>

GRASER, A., WEISSENFELD, A., HEISTRACHER, C., DRAGASCHNIG, M., & WIDHALM, P. (2024). Federated learning for anomaly detection in maritime movement data. *2024 25th IEEE International Conference on Mobile Data Management (MDM)*, 77–82. <https://doi.org/10.1109/MDM61037.2024.00030>

GRÄUPL, T., REISENBAUER, A., HECKO, M., RASOULI, A., GRASER, A., DRAGASCHNIG, M., WEISSENFELD, A., DEJAGERE, G., & SAKR, M. (2025). Federated learning and trajectory compression for enhanced AIS coverage. *2025 Symposium on Maritime Informatics and Robotics (MARIS)*, 1–4. <https://doi.org/10.1109/MARIS64137.2025.11139533>

GRIGOROPOULOS, G., TROUPIOTIS-KAPELIARIS, A., CHAMATIDIS, I., FILIPPOU, E., & BERETA, K. (2025, March 14). Transforming Maritime Safety: Data-driven Applications for the Real-Time Detection and Mitigation of Maritime Incidents. *Session*

*Demo. Proceedings of the 28th International Conference on Extending Database Technology (EDBT), 25-28 March, 2025, Barcelona, 1070-1073.* <https://www.open-proceedings.org/2025/conf/edbt/paper-308.pdf>

GRPC. (2026). Grpc. <https://grpc.io/>

HOGG, K., BUZZI, A., CLAUDET, J., COMPAIN, N., DAMALAS, D., DI LORENZO, M., GALLI, S., GIAKOUMI, S., SALINAS-AKHMADEEVA, I., SGARDELI, V., RUSSO, T., SCIANNA, C., TSERPES, G., & DI FRANCO, A. (2024). *Mapping of MPAs and their associated fishing activities in the Mediterranean and Black Seas (MAPAFISH-MED)*. Publications Office of the European Union. [https://iris.cnr.it/retrieve/3413e841-40dd-4af5-bf99-a45333c11485/MAPA-FISH\\_MED\\_compressed.pdf](https://iris.cnr.it/retrieve/3413e841-40dd-4af5-bf99-a45333c11485/MAPA-FISH_MED_compressed.pdf)

IDIBEZKODA, F. (2024). The evolution of environmental diplomacy: reviewing four decades of research. In A. Sharifi, J. L. Candelaria, D. Simangan, & S. Kaneko (Eds.), *Navigating peace and sustainability in an increasingly complex world* (pp. 241–257). Springer Nature Singapore. [https://doi.org/10.1007/978-981-97-8772-2\\_12](https://doi.org/10.1007/978-981-97-8772-2_12)

IUCN Joint SSC/WCPA Marine Mammal Protected Areas Task Force. (2025). *Global dataset of Important Marine Mammal Areas (IUCN IMMA)* (April 2026 release) [Data set]. IMMA e-Atlas. <https://marinemammalhabitat.org/imma-eatlas/>

KAPIDANI, N., ASTYAKOPOULOS, A., BOLAKIS, C., MOUTZOURIS, M., HAJDUCH, G., VOSINAKIS, G., SCRIMA, P., & PALADIN, Z. (2022). Maritime information sharing environment deployment using the advanced multilayered Data Lake capabilities. *Pomorstvo*, 36(2), 291–304. <https://doi.org/10.31217/p.36.2.13>

KINACIOGLU, M. (2023). Militarized governance of migration in the Mediterranean. *International Affairs*, 99(6), 2423–2441. <https://doi.org/10.1093/ia/iaad232>

KUMAR, A. (2026). Weaponising the supply chain: yemen's blockade and the contradictions of maritime logistics capital. *Antipode*, 58(1). <https://doi.org/10.1111/anti.70107>

MATIJEVIĆ, S. (2021). Pollution from Fish Farming Activities in the Adriatic Sea. In D. Joksimović, M. Đurović, I. S. Zonn, A. G. Kostianoy, & A. V. Semenov (Eds.), *The montenegrin adriatic coast: marine chemistry pollution* (Vol. 110, pp. 373–394). Springer International Publishing. [https://doi.org/10.1007/978-2020\\_697](https://doi.org/10.1007/978-2020_697)

MERCATOR OCEAN INTERNATIONAL (2025). Copernicus Marine Service. Mercator Ocean International. <https://www.mercator-ocean.eu/about-us/mercator-ocean/what-we-do/copernicus-marine-service/>

MIHAILOVIC, A., KAPIDANI, N., LUKSIC, Z., TOURNIER, R., VELLA, G., MOUTZOURIS, M., DE SOUSA, B., BLUM, A., & PALADIN, Z. (2022). Planning a Case for Shared Data Retrieval across the European Maritime Common Information

Sharing Environment. *2022 26th International Conference on Information Technology (IT)*, 1–6.

<https://doi.org/10.1109/IT54280.2022.9743531>

MITZEN, J. (2006). Ontological security in world politics: state identity and the security dilemma. *European Journal of International Relations*, 12(3), 341–370.

<https://doi.org/10.1177/1354066106067346>

MOUSSAOUI, M., & RACHID, A. (2023). Building bridges through science diplomacy in the mediterranean: speaking a common language. In M. Moussaoui (Ed.), *Global science's cooperation opportunities, challenges, and good practices* (pp. 118–147). IGI Global. <https://doi.org/10.4018/978-1-6684-7874-5.ch006>

NATIONAL GEOGRAPHIC PRISTINE SEAS. (2026). *Marine biodiversity* [ArcGIS imagery layer]. ArcGIS.

[https://tiledimageservices.arcgis.com/P3ePLMYs2RVChkJx/arcgis/rest/services/210923e\\_biodiversity\\_ranking\\_WM\\_1000\\_masked\\_mrf\\_lerc/ImageServer](https://tiledimageservices.arcgis.com/P3ePLMYs2RVChkJx/arcgis/rest/services/210923e_biodiversity_ranking_WM_1000_masked_mrf_lerc/ImageServer)

OCEANOBS. (n.d.). *monGOOS Data Center*. Oceanobs. Retrieved April 10 2026 from <http://oceanobs.mongoos.eu/>

RAI, A. (2025). Turbulent waters in the red sea: understanding maritime shipping business impacts and implications. *Journal of Transportation Security*, 18(1), 17.

REMPEC REGIONAL MARINE POLLUTION EMERGENCY RESPONSE CENTER FOR THE MEDITERRANEAN SEA. (2022). *Study on trends and outlook of marine pollution*. REMPEC.

<https://www.rempec.org/en/knowledge-centre/online-catalogue/etudetendances2022.pdf/view>

RICCABONI, A., SACHS, J., CRESTI, S., GIGLIOTTI, M., & PULSELLI, R. M. (2020). *Sustainable development in the Mediterranean. Report 2020*. Sustainable Development

SOLUTIONS NETWORK MEDITERRANEAN (SDSN Mediterranean).

<https://aifm.org/en/resources-en/the-2020-report-on-sustainable-development-in-the-mediterranean-has-just-come-out-2/>

SIMONCELLI, S., VERNET, M., & COATANOAN, C. (2024). *International Conference on Marine Data and Information Systems - Proceedings Volume*. Istituto Nazionale Di Geofisica e Vulcanologia (INGV). <https://doi.org/10.13127/misc/80>

SZENTIVANYI, N. (2024). *The Impacts of the Red Sea Shipping Crisis*. J.P. Morgan. <https://www.jpmorgan.com/insights/global-research/supply-chain/red-sea-shipping>

FAO (2020). *The state of mediterranean and black sea fisheries 2020*. FAO. <https://doi.org/10.4060/cb2429en>

UNEPMAP. (n.d.). *Barcelona Convention and Amendments*. UNEPMAP. Retrieved April 10 2026 from <https://www.unep.org/unepmap/who-we-are/contracting-parties/barcelona-convention-and-amendments>

UNEP. (1976) *Convention for the Protection of the Marine Environment and the Coastal Region of the Mediterranean*. UNEP.

UNEPMAP. (2016). *Mediterranean Strategy for Sustainable Development 2016-2025 - Investing in environmental sustainability to achieve social and economic development*. UNEPMAP.  
[https://planbleu.org/sites/default/files/publications/mssd\\_2016-2025\\_final.pdf](https://planbleu.org/sites/default/files/publications/mssd_2016-2025_final.pdf)

VASILEVA, B., & AHMED, M. (2020). The Concept of the European Maritime Single Window Environment for Simplified Digital Information System, Introduced by the Regulation (EU) 2019/1239. *Centre for Studies in European Integration Working Papers Series*, 16, 36–39. <https://www.ceeol.com/search/article-detail?id=941908>

ZAKZOUK, M., ABDULAZIZ, A. M., ABOU EL-MAGD, I., DAHAB, A. S., & ALI, E. M. (2025). Automated oil spill detection using deep learning and SAR satellite data for the northern entrance of the Suez Canal. *Scientific Reports*, 15(1), 20107–20125.

# eur@mesco

Policy Study