EUROPEAN DEFENCE AGENCY

FACTSHEET
www.eda.europa.eu

Protection of offshore critical energy infrastructure beyond national sovereignty: military rules of engagement and barriers

Background

In 2024, the European Union navigates through a complex and volatile geopolitical and security context, prompted by the invasion of Ukraine, the overlapping energy crisis and the first attacks on its **offshore critical energy infrastructure (OCEI).** Europe's maritime areas have become hotspots of ongoing warfare, zones of security alert due to their proximity to regional conflicts, places of presumed deliberate attacks on subsea pipelines and cables, and areas of intensified espionage activities around offshore energy installations.

An unprecedented proliferation of physical, cyber and hybrid risks, threats and vulnerabilities acting in synergy, as well as a plethora of state-led, state-sponsored, private, non-state and transnational actors, concur and pose pressure on the security and resilience of the European OCEI.

Scope and Objectives

In this context, this research study has been developed in the context of the Working Group 3 on 'Protection of Critical Energy Infrastructure' of the Consultation Forum for Sustainable Energy in the Defence and Security Sector (CF SEDSS), as an effort to:

1. Identify an up-to-date set of existing and emerging **security risks, threats and vulnerabilities for the OCEI** in the EU;
2. Provide an overview of the complex **legal regime governing the OCEI** to highlight the opportunities and the limits of engagement for the ministries of defence (MoDs) to protect the offshore critical energy infrastructure in the EU;
3. Provide key **recommendations and guidelines for policy update and development** that would integrate all the relevant OCEI under an integrated policy umbrella, as well as for adopting **security-enhancing measures for the protection of OCEI** in the EU.

Problem Analysis

Europe has been experiencing, particularly after February 2022, the emergence and the proliferation of new fast-evolving **security risks, threats and vulnerabilities** to the OCEI in all four major maritime regions of the EU (the North Sea-Atlantic region, the Baltic Sea, the Black Sea and the Mediterranean Sea). In these maritime regions, disputes over rights to exploit offshore natural resources like natural gas are common. Since 2022, there has been a rise in military activity, including contested zones and mine placements, threatening offshore exploration safety. Additionally, offshore infrastructures face cybersecurity threats and hybrid warfare tactics. Thus, the study outlines current threats, risks, and vulnerabilities to the safety of EU Offshore Critical Energy Infrastructure (OCEI) in both conventional and hybrid scenarios.

EUROPEAN DEFENCE AGENCY | European Defence Energy Network

This project has received funding from the European Union's Horizon 2020 research and innovation programme under grant agreement No 882171

The **legal regime** of the critical offshore energy infrastructure represents a complex web of national and international law provisions, raising questions regarding the legal aspects related to sovereignty, sovereign rights, and jurisdiction over the OCEI. The study thus provides an overview of the major challenges stemming from the complex and, at times, ambiguous legal regime governing the OCEI, shedding light on the opportunities but also on the limits of engagement for the military to protect the offshore critical energy infrastructure.

Solution Implementation and Way Ahead

The offshore critical energy infrastructure exhibits specific vulnerabilities compared to the onshore infrastructure, stemming from its location and geography, environmental and weather conditions, as well as legal regimes, that require a different protection, security and defence approach compared to the onshore infrastructure. **Fragmentation and interdependencies represent nonetheless the main challenges to the effective protection of the OCEI.**

Enhancing the resilience of the CEI is key to the overall European security facing an unprecedented escalation of risks, threats and vulnerabilities in the current geopolitical context. For this purpose, the study aims to bring together an aggregated set of **recommendations and guidelines** intended to identify key actions at EU-level for reinforcing the protection and resilience of OCEI.

1. EU-level recommendations and guidelines:

To **reduce the fragmentation** at policy and actors' level, the study proposes to:

- Develop an aggregated EU-level OCEI Security Strategy for all types of OCEI an all-hazard approach, under a single policy umbrella;
- Establish a comprehensive OCEI Forum at EU-level reuniting MoDs and OCEI stakeholders;
- Develop an EU-standardised methodology to evaluate reliance on OCEI and identify risks, threats and vulnerabilities;
- Establish an EU-level Observatory for OCEI Risk Assessment with the joint participation of the MoDs and civilian experts.

To address the critical interdependency between the large variety of entities active in the OCEI field, the study suggests to:

- Create an EU-level information disclosure and sharing mechanism for countering physical, cyber and hybrid attacks;
- Create a practice-sharing framework composed of an incident-triggered technical task force;
- Develop contingency plans and tabletop simulation exercises bringing together relevant stakeholders from all parts of the sector;
- Keep track of ownership of defence-related OCEI.

2. MoDs-level recommendations and guidelines:

There are several areas of action where **the MoDs could make a positive contribution to the protection of the OCEI,** having in view the fact that technological developments pertaining to the security and protection of the maritime and subsea infrastructure must be adapted and upgraded to keep pace with the capabilities of potential adversary actors. Thus, the study identifies the need to:

- Enhance maritime security and protection of OCEI with updated technology, such as unmanned surface vehicles (USV), autonomous underwater vehicles (AUVs) and unmanned aerial systems (UAS) for intelligence and reconnaissance missions, incident detection, mine location and anti-submarine warfare;
- Boost training, upskilling and reskilling of defence personnel, including through the cooperation between military and civilian academia;
- Establish a hybrid actions reaction team for preventing and countering attacks on OCEI;
- Conduct, on a regular basis, vulnerability assessments to improve situational awareness and mitigate risks in case of threats against defence-related OCEI;
- Develop or update plans for the prevention, preparedness, response and recovery necessary to maintain the resilience of defence-related OCEI against physical, cyber and hybrid threats;
- Increase the use of the artificial intelligence, as AI enabled systems will have a significant role in information control and counterintelligence activities;
- Perform real scenario-based exercises, simulations and tabletop exercises;
- Cooperate with the industry and academia in order to take advantage of the existing advanced research and innovations in underwater robotics for extended monitoring and surveillance of the offshore and submarine infrastructure.

This project has received funding from the European Union's Horizon 2020 research and innovation programme under grant agreement No 882171