HYBRIDMAR

Operational identification and attribution of shadow fleet as a resilience instrument for European maritime critical infrastructure and strategic chokepoints under hybrid threats

Purpose and overall approach

HYBRIDMAR is conceived as a Horizon Europe Cluster 3 Innovation Action aimed at developing and validating a European civil capability for the operational identification and attribution of shadow fleet activities as a key vector of hybrid threats.

Despite the growing relevance of shadow fleet activities as a key enabler of hybrid threats in the maritime domain, no integrated European capability currently exists to identify, assess and operationally attribute these activities in a consistent and actionable manner. Information remains fragmented across national authorities, EU agencies and commercial intelligence providers, each operating within their own systems and mandates. As a result, available data does not translate into a shared operational picture, and decision-making is based on partial evidence and non-standardised criteria. This gap is not technological but structural: Europe lacks a common framework that transforms dispersed data into defensible identification, attribution and action protocols applicable to maritime critical infrastructure and strategic chokepoints.

The project addresses a structural gap in the European maritime security architecture: while multiple actors generate partial intelligence, no integrated system currently exists to identify, assess and attribute shadow fleet operations in a way that supports operational decision-making.

Building on the present concept note, the project extends an existing and well-established European operational logic —Port State Control— into a domain where no equivalent structured system exists today. The objective is to deliver a **deployable operational capability** that enables authorities to act.

Strategic positioning

The proposal is positioned at the intersection of maritime security, protection of critical infrastructure and hybrid threats. It responds directly to recent developments affecting subsea infrastructure, energy systems and strategic maritime routes, where infrastructure and chokepoints overlap geographically and concentrate risk exposure.

The concept of shadow fleet is treated not as an isolated phenomenon but as a **systemic operational platform** enabling multiple threat vectors, including sanctions evasion, covert logistics, infrastructure interference and operational reconnaissance. Addressing this vector provides leverage across several policy priorities simultaneously.

HYBRIDMAR aligns with the revised EU Maritime Security Strategy and the Critical Entities Resilience Directive, and contributes across multiple policy areas within Cluster 3, including maritime security, resilient infrastructure and organised crime.

Concept and methodology

The project develops a European system capable of responding, for a given vessel or event, to three operational questions: whether it can be classified as part of the shadow fleet and with what level of confidence; to which operational network or jurisdiction it may be attributed; and which action is recommended for the competent authority.

This capability is built through a structured **methodological approach** articulated across six work packages.

The initial phase focuses on the development of an operational taxonomy of shadow fleet, translating observable indicators—related to vessel identity, ownership, behaviour and operational patterns—into a structured classification system analogous to the Paris MoU deficiency model. This work requires strong academic leadership in maritime security, regulatory frameworks and risk modelling, in close interaction with operational stakeholders.

The core of the project lies in the development of an interoperable system integrating heterogeneous data sources, including AIS, satellite data, institutional systems and commercial maritime intelligence. This layer constitutes the main technological component of the project and requires the leadership of a technology partner with demonstrated capacity in data integration, system architecture and platform development. The system is conceived as an analytical layer compatible with existing European infrastructures, rather than a replacement.

On this basis, the project develops an early warning capability focused on the detection of anomalous behaviours in proximity to maritime critical infrastructure and strategic chokepoints. This component builds on the integrated system and combines data analytics, behavioural modelling and operational criteria defined with end-users.

Validation is carried out in multiple European maritime contexts, covering different types of chokepoints and infrastructure configurations. This phase is led by operational partners, including maritime authorities, coast guards and port authorities, ensuring that the system responds to real operational needs and constraints.

The final phase translates project results into doctrine, training and policy recommendations, establishing a pathway towards adoption at EU and Member State level. It includes the development of training curricula for operational actors and a structured set of recommendations for integration into existing regulatory and operational frameworks, including potential pathways to innovation procurement.

The project is designed as a civil initiative based exclusively on open, institutional and commercial data. Actors with access to classified information may contribute through validation mechanisms without compromising data sensitivity, ensuring a bridge between civil analytical capacity and operational realities.

Consortium approach

The consortium is being structured to combine complementary capacities required to deliver an operational system of this nature.

The academic core builds on maritime universities, including partners within the SEA-EU alliance, providing expertise in maritime systems, risk modelling and regulatory frameworks. This is complemented by specialised research centres in security and data analysis.

A central role is assigned to technology partners responsible for system architecture, data integration and platform development. Their contribution is critical to achieving the required level of technological maturity and interoperability.

Operational stakeholders are integrated as full partners, not only as validators but as co-designers of the system. This includes maritime authorities, coast guards, port authorities and law enforcement bodies, ensuring alignment with operational needs.

The consortium is further strengthened by the inclusion of maritime intelligence providers, legal experts in maritime regulation, and organisations contributing to policy and strategic analysis. The project benefits from a strong ecosystem involving naval, law enforcement and port authorities, as well as major industrial actors in the maritime sector, providing a solid foundation for validation and deployment.

The target configuration is a consortium of approximately 12 to 14 beneficiaries from at least seven countries.

Duration, budget and implementation framework

The project is designed with a duration of **36 months**, consistent with the requirements of an Innovation Action.

The expected EU contribution is approximately **€4.5 million**, in line with the indicative budget of the topic. The budget distribution follows the logic of the work plan, with a significant share allocated to system development and integration, and dedicated resources for validation, operational engagement and uptake.

Work packages related to system architecture and data integration represent the largest share of the budget, reflecting the technological core of the project. Validation activities, involving multiple operational environments, also require substantial allocation. Management, coordination and policy uptake components are structured to ensure coherence, quality and long-term impact.

Expected impact

HYBRIDMAR is expected to deliver a concrete operational capability enabling European authorities to identify and respond to hybrid threats in the maritime domain with a level of integration and attribution not currently available.

By addressing shadow fleet as a systemic vector, the project contributes to reducing the operational capacity of multiple threat types simultaneously. It enhances situational awareness, supports decision-making and strengthens the resilience of critical infrastructure.

The project also provides a replicable methodological framework and contributes to policy development, training and future European initiatives in maritime security.

Next steps and partner engagement

The project is currently in a structuring phase. Potential partners are invited to engage in the co-design process, particularly in relation to system architecture, data integration, validation scenarios and operational use cases.

Discussions will focus on aligning partner expertise with project needs, defining roles within the consortium and ensuring coherence with the expectations of the Horizon Europe call.