BLUE CLUSTER

Feasibility Study

Ecosystem development for critical maritime infrastructure protection

October 2025

Executive Summary

This feasibility study, commissioned by the Belgian Ministry of Defence (MoD) and conducted by Blue Cluster, explores the creation of a mission-driven Research, Technology, and Innovation (RTI) ecosystem focused on Critical Maritime Infrastructure Protection (CMIP). The study aligns with the MoD's Defence, Industry and Research Strategy (DIRS), which aims to strengthen Belgium's defence technological and industrial base by promoting research, development and innovation in collaboration with external partners, i.e. the industry and research and technology organisations (RTOs). It focuses on enhancing national security and positioning Belgium as a competitive partner in European capability development.

BACKGROUND AND RATIONALE

Critical Maritime Infrastructure (CMI) encompasses essential assets in offshore energy, communication, and ports, which are increasingly targeted by hybrid warfare and grey zone threats—state-sponsored disruptive actions below the threshold of military action. Given the socio-economic importance and vulnerability of these assets, there is a pressing need to enhance their protection through innovation in surveillance, detection, response, communication, data exchange, and repair technologies.

STUDY OBJECTIVES AND APPROACH

The study's primary objective is to assess the feasibility of establishing a sustainable, collaborative innovation ecosystem that accelerates the development and deployment of dual-use technologies to protect Belgium's maritime infrastructure. The methodology integrates foresight, stakeholder engagement, ecosystem mapping, governance design, financial modelling, and communication planning. It employs a mixed-methods approach combining quantitative data analysis with qualitative insights from industry, research, and government stakeholders.

APPLIED ECOSYSTEM MISSION AND VISION

The proposed CMIP innovation ecosystem's mission is to drive innovation as a catalyst for protecting Belgium's critical maritime infrastructure by connecting diverse stakeholders in a collaborative network. The vision is to position Belgium as an international leader in resilient, secure, and smart maritime domains by 2050, leveraging AI-enabled, interoperable solutions and fostering economic growth and strategic partnerships at national, European and NATO level.

MARKET AND TECHNOLOGY LANDSCAPE

The study identifies strong market drivers, including increasing hybrid threats and public investments in maritime security. Belgium's robust scientific and technological foundation, supported by world-class universities, research centres, and innovation hubs, provides a fertile ground for ecosystem development. Technologies span sensors, autonomous drones, digital twins, automated systems and robotics, secure communications, and advanced analytics.

STAKEHOLDER ENGAGEMENT AND VALUE DRIVERS

Extensive stakeholder consultations reveal strong buy-in from industry, SMEs, start-ups, research institutions, and government agencies. Key value drivers include network building, knowledge exchange, collaborative innovation, scaling and valorisation, internationalisation and policy development. The ecosystem aims to support SMEs and start-ups through dedicated services and access to innovation financing, fostering a vibrant "ecosystem of ecosystems."

GOVERNANCE AND MANAGEMENT

A clear governance framework is proposed, including an ecosystem board, steering group, scientific advisory, and SME representation to ensure transparency, efficiency, and inclusiveness. A phased roadmap guides the ecosystem's development from initial setup to full operational maturity, with mechanisms for identifying research priorities and managing project pipelines.

FINANCIAL MODEL AND SUSTAINABILITY

The study outlines a sustainable financial model combining public funding, private investment, and innovation financing instruments. Resource estimates cover ecosystem management, RTDI activities, and communication efforts, ensuring long-term viability.

COMMUNICATION AND COMMUNITY ENGAGEMENT

A strategic communication plan targets key audiences to increase ecosystem visibility, foster stakeholder engagement, and promote collaborative innovation culture.

RECOMMENDATIONS AND CONCLUSIONS

This feasibility study intends to assess whether establishing an innovation ecosystem for Critical Maritime Infrastructure Protection (CMIP) in Belgium is both necessary and achievable. The analysis was guided by two fundamental questions: "Do we have all the dots?", do we have the essential assets, capabilities, and stakeholders, and "Can we connect the dots?", do we have the ability to integrate these elements into a functioning, value-creating innovation ecosystem.

DO WE HAVE ALL THE DOTS?

Our study demonstrates that Belgium possesses a robust foundation for ecosystem development:

- There is a critical mass of engaged industry partners, technology companies, research institutions, government agencies, and innovation hubs with proven expertise in maritime security, digital technologies, and dual-use innovation;
- The technology landscape includes mature capabilities in surveillance, detection, secure communications, autonomous systems, data analytics, and digital twins, supported by ongoing R&D and pilot projects;
- The growing threat landscape, strong public investment, and alignment with national and European security strategies create a foundation for ecosystem growth;
- There is a demonstrated willingness among stakeholders to collaborate, share knowledge, and pursue joint value creation, as evidenced by existing clusters, networks, and successful collaborative projects.

CAN WE CONNECT THE DOTS?

The study further establishes that the necessary mechanisms and conditions exist to integrate these assets into a cohesive, high-impact ecosystem:

- A clear governance structure, with defined roles for coordination, scientific guidance, and SME representation, has been proposed and validated through stakeholder consultation;
- Processes for project selection, priority setting, technology transfer, valorisation and stakeholder engagement are well-defined and align with best practices from peer EU ecosystems;
- A sustainable financial model, leveraging both public and private funding sources, has been mapped out to support ecosystem management and innovation activities;
- The ecosystem is designed for openness and interoperability, with strong potential for both national and international partnerships, ensuring access to complementary expertise and markets;
- A phased implementation plan provides clear steps for ecosystem launch, growth, and maturity, reducing risk and ensuring adaptability.

RECOMMENDATIONS

1. Launch a mission-driven "Made in Belgium" innovation ecosystem to accelerate the valorisation of the dual-use market and international upscaling;
2. Create an open collaboration with defence and develop an aligned innovation roadmap;
3. Unite scientific and research communities with start-ups, innovative SMEs, and corporates to strengthen knowledge and provide access to top expertise and talent;
4. Provide access to transparent, lightweight and fast-track innovation funding and financing;
5. Develop a lead role in a European "ecosystem of ecosystems" and consortium development for EU and international funding;
6. Prioritise the integration of start-ups and SMEs in (defence) system solutions; leverage champions to become global leaders in the CMIP market;
7. Develop tailor-made value-added services for SMEs and start-ups;
8. Facilitate access to living labs and test infrastructure to speed up innovation processes;
9. Leverage on securing port critical infrastructure with ports as a unique innovation platform for internationalisation;
10. Ensure an Ecosystem Management Organisation governance structure which is independent, agile, and transparent and links to regional and local initiatives;
11. Set up a task force on interoperability;
12. Promote economic and societal value of CMI protection with civil society and policy-makers.

In addition to these recommendations, this study suggests to develop high impact projects on:

- Real-time maritime situational awareness (digital twin) of the Belgian North Sea;
- Belgium's niche expertise in drones (UAV, USV, AUV) and valorise its export potential;
- The development of repair capacity to create a first-mover advantage.

FINAL ASSESSMENT

Based on the evidence gathered, this study concludes that the creation of a CMIP innovation ecosystem in Belgium is both feasible and strategically justified. Belgium not only has all the necessary "dots", i.e. the assets, stakeholders, and capabilities, but also the means and motivation to connect them effectively. The preconditions for successful ecosystem building are present: a shared mission, a critical mass of expertise, enabling policies, and a clear organisational and financial framework.

Moving forward, Belgium is well positioned to establish a future-ready, internationally connected innovation ecosystem that will enhance the protection of critical maritime infrastructure, drive economic growth, and reinforce national and European security objectives.

Table of Contents

Executive Summary 1

Table of Contents 4

1 Introduction and study objectives 6
- 1.1 Introduction and background 6
- 1.2 Definition of Critical Maritime Infrastructure 6
- 1.3 Research, Techology and Innovation (RTI) Ecosystem Feasibility Approach 9

2. Methodological approach 11
- 2.1. Study timeline and phases 11
- 2.2. Mixed methods approach 12

3. Ecosystem mission and vision 15
- 3.1. Mission 15
- 3.2. Vision 15
- 3.3. Strategic foresight 16

4. Market 20
- 4.1. Market drivers and macro trends 20
- 4.2. Market dynamics and public investment 20
- 4.3. Security value 21

5. Technology mapping, stakeholder landscape and the voice of the stakeholders 25
- 5.1. Technology and stakeholder mapping 25
- 5.2. Our strong foundation in science, technology research and innovation 31
- 5.3. Stakeholders perspective on an RTI ecosystem 34
- 5.4. Priority ranking of RTI-ecosystem value drivers by respondents 37
- 5.5. Buy-in of stakeholders 38

6. Value drivers and services of the ecosystem 40
- 6.1 CMIP ES services portfolio 40
- 6.2 Specific focus on SMEs, start-ups and scale-ups 47
- 6.3 Ecosystem of ecosystems 53
- 6.4 Access to innovation financing instruments 57

7 Recommendations & conclusions 61

8 Annexes 62

Annex 1: List of abbreviations and acronyms 63

Annex 2: Strategic actions on the CMIP recommendations 65

Annex 3: Market size and growth projections for CMIP 70

1. Introduction and study objectives

1.1 Introduction and background

In 2022, the Ministry of Defence developed a long-term strategy to enhance national security and position **Belgium as a competitive partner** in European capability development. The Defence, Industry and Research Strategy (DIRS) of the Ministry of Defence (MoD) intends to strengthen Belgium's defence technological and industrial base by promoting research, development and innovation in collaboration with external partners, i.e. the industry and research and technology organisations (RTOs). It aims to position defence as a strategic growth engine for the Belgian economy, while simultaneously fostering the development of specialised knowledge and strengthening execution capacity in key technological and operational domains. The Royal Higher Institute for Defence (RHID) plays a key role in the implementation of the DIRS strategy.

The MoD explores the development of **mission-focused innovation ecosystems** as important tools in the DIRS framework. A mission-driven innovation ecosystem is a network of diverse stakeholders, including companies, knowledge and research institutions, government agencies and other organisations, working together towards a common goal (mission) to promote new technologies, entrepreneurship and economic growth. Two focus areas of the ecosystem's mission have been prioritised: protection of critical maritime infrastructure and cyber and digital security.

Given Blue Cluster's role and track record in promoting collaborative research and innovation and ecosystem development in the Blue Economy, the MoD commissioned Blue Cluster to conduct a feasibility study to support decision-making on the development of an innovation ecosystem focused on the protection of critical maritime infrastructure (CMIP ES).

1.2 Definition of Critical Maritime Infrastructure

The Critical Entities Resilience (CER) Directive (EU 2022/2557) significantly broadens and strengthens the EU's approach to protecting critical infrastructure. It moves beyond the previous, more limited focus of the 2008 European Critical Infrastructure Directive. The CER Directive's core is not just about the physical assets themselves, but about the "critical entities" (public or private organisations) that provide "essential services". Critical infrastructure is defined in relation to these services as: "an asset, a facility, equipment, a network or a system, or a part of an asset, a facility, equipment, a network or a system, which is necessary for the provision of an essential service". An essential service is defined as "a service which is crucial for the maintenance of vital societal functions, economic activities, public health and safety, or the environment." This broad definition ensures that the scope covers services fundamental to the well-being and functioning of society.

The spectrum of maritime infrastructures is broad and includes among others transport, energy, fishing, communication and ecosystems related systems and assets on sea, under sea and on land. In the context of this feasibility study, Critical Maritime Infrastructure (CMI) includes in particular the critical infrastructure under and on the water in the areas of **energy** (offshore platforms, power cables, pipelines), **communications** (data cables and connectors, transmission towers) and **ports** (maritime access, locks and docks).

Not all maritime infrastructure in these areas is critical as this depends primarily on the following parameters:

- Socio-economic impact of an outage or structural damage of infrastructure including its geographic extent (international, nation-wide or more localised), the potential gravity of the disruption, the subsequent direct and indirect economic and financial losses and exposure to other risks in terms of security, safety or societal context;
- Level of redundancy in the overall system;
- Complexity, cost and duration to restore, repair or replace the infrastructure.

Belgium, like all EU Member States, is in the process of identifying "critical entities" under the CER Directive (EU 2022/2557), due for July 2026. As of now, there isn't a publicly available, definitive, and finalised list of all critical infrastructure, specifically within the maritime context

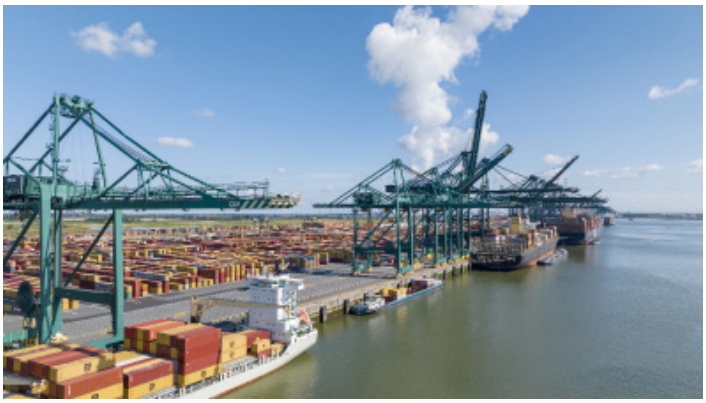
.



Important transmission connectors such as the modular offshore grid (MOG) connecting four offshore wind parks to the Stevin landing substation, the subsea Nemo Link between Belgium and the UK and the Princess Elisabeth energy island (under construction) will certainly be part of the list of critical infrastructure.

The Zeebrugge LNG terminal (major hub for import, storage, and distribution across Western Europe) and the Western Scheldt[1] as well as important locks such as the Berendrecht or Kieldrecht locks (access lifeline of the Port of Antwerp-Bruges) are obviously CMI.

Although the subsea network of data communication cables has more in-built redundancy in comparison with oil and gas pipelines, recent incidents in the Baltic Sea end 2024 demonstrate substantial negative impact and disruption caused by a cluster of incidents and damage on multiple data cables.



1 Although the Western Scheldt is not considered infrastructure in the strict sense, it connects North Sea Port and the Port of Antwerp to the North Sea, and its navigability for the ever-growing size of cargo ships is continually maintained through dredging.

For the scope of the proposed CMIP ES, it is therefore recommended to apply a broad interpretation of CMI to cover the protection and security of all relevant maritime infrastructure and related systems in the energy, communications and transport (i.e. ports) domains. Although boats and ships are not considered as CMI in itself, their surveillance will be important in the context of threat identification and CMI protection.



There are various ways to categorise the CMI threat landscape, e.g. intentional versus unintentional damage, type of perpetrator, etc. Based on Bueger's threat spectrum overview above, the mission of the ecosystem will primarily focus on deterrence, detection and identification of threats related to hybrid threats and grey zone warfare and terrorist threats.

Hybrid threats and **grey zone warfare** refer to state disruptive actions that fall below the threshold of direct military action and are often difficult to attribute directly to a foreign government. Unintentional damage from natural disasters and accidents and intentional damage from blue crimes and acts of war are important, but currently fall outside the scope of the MoD's ecosystem mission.

1.3 Research, Technology and Innovation (RTI) Ecosystem Feasibility Approach

In a Research, Technology and Innovation (RTI) ecosystem, various actors and stakeholders collaborate in a targeted manner, driven by a shared mission, vision and strategy. This collaboration needs to create added value for all parties involved and provides direction to the research, development and innovation agenda across the participants in the ecosystem.

Experience in many other sectors in Belgium and internationally shows that the creation of thematic ecosystems strengthens collaborative efforts and stimulates research, development and innovation due to enhanced interdisciplinary interaction. This ecosystem environment improves knowledge sharing and has the potential to accelerate innovation and valorisation.

ECOOM (Expertise Centre for Research and Development Monitoring in Flanders) in collaboration with KU Leuven and VIVES has conducted research on the impact of collaborative research within clusters on the productivity growth of companies.[1] The study provides empirical evidence that participation in organised cluster initiatives, particularly those focused on collaborative R&D like the Flemish Spearhead Clusters, can lead to enhanced productivity (between 1-4.4% Total Factor Productivity) among member companies. This suggests that the "cluster effect" (e.g. through knowledge spillovers, shared resources, access to specialised labor, and facilitated collaboration) translates into tangible economic benefits for individual firms, beyond just innovation output.

The establishment of such thematic ecosystems for defence-related and dual-use technologies and systems is an effective policy approach to contribute to the achievement of the overall objectives of the DIRS. By supporting such ecosystems, the Ministry of Defence contributes to the development of the technological and industrial fabric. Ultimately, the ecosystem is expected to evolve into a self-sustaining and viable collaborative network to autonomously support further research and development, specifically focused on defence and dual-use technologies and applications.

This feasibility study supports future decision making regarding the initiation and support of a CMI ecosystem within the DIRS framework:

- Understanding the ecosystem, including mapping the ecosystem participants, their interest, expectations and commitment to such an ecosystem;
- Organisation of ecosystem management, including strategy, governance and action plan;
- Ecosystem management costs and funding, including R&D and innovation funding.

2 Angelino, P., Czarnitzki, D., & Volckaert, A. (2023). Do cluster initiatives boost productivity? The impact of cluster membership on firm level productivity. VLAIO.

CONCLUSION

The Belgian Ministry of Defence (MoD), through its Defence, Industry and Research Strategy (DIRS), aims to strengthen national security and technological autonomy by promoting mission-driven research, development, and innovation in collaboration with industry and research institutions. The DIRS strives to position defence as a strategic growth engine for the Belgian economy, while simultaneously fostering the development of specialised knowledge and strengthening execution capacity in key technological and operational domains. The Royal Higher Institute for Defence (RHID) plays a central role in implementing this strategy. A key focus is the development of innovation ecosystems, prioritising two domains: protection of critical maritime infrastructure (CMI) and cyber and digital security.

To explore the feasibility of a CMI-focused innovation ecosystem, the MoD commissioned Blue Cluster, leveraging its expertise in fostering collaborative innovation within the blue economy. CMI encompasses vital maritime infrastructure related to energy, communication, and port operations, including assets located at sea, underwater, and on land. Infrastructure is classified as "critical" based on socio-economic impact, system redundancy, and restoration complexity.

The proposed ecosystem will primarily focus on detecting, deterring, and identifying hybrid and grey zone threats - state-sponsored disruptive actions that fall below the threshold of military action. Accidental damage or acts of war are currently outside the ecosystem's scope.

The feasibility study consists of three main components: (1) mapping and engaging stakeholders in the ecosystem, (2) defining governance structures, strategy, and action plans, and (3) estimating costs and identifying funding sources for ecosystem management and innovation activities. The ultimate goal is to establish a sustainable, collaborative innovation network advancing defence and dual-use technologies within the DIRS framework.

2. Methodological approach

2.1 Study timeline and phases

The feasibility study was carried out in five sequential work packages.

Vision, Mission and Strategy

Comprehensive analysis of technological developments and the future outlook of the ecosystem. Key topics included:

- Defining vision, mission, and strategy;
- Identifying trends, risks, and drivers;
- Foresight;
- From prioritisation to roadmap development;
- From innovation roadmap to an innovation programme with an action plan;
- From innovation programme to concrete project development.

Governance and Management

Research into the legal framework and governance model that ensures the efficiency and transparency of the ecosystem. This included:

- Setting up the governance model for the ecosystem;
- Governance model for individual projects;
- Developing a process for performance monitoring.

Ecosystem Development and Stakeholder Engagement

Identifying and involving relevant stakeholders. This phase explored how to expand and strengthen the ecosystem. It included:

- Mapping the ecosystem at Belgian and European level;
- Analysis of the technological landscape;
- Ensuring buy-in from companies and strategic partners (knowledge institutions), with particular attention to SMEs;
- Value chain analysis, in relation to innovation roadmaps.

Financial Model

Development of a sustainable financial model that can support the ecosystem and its projects in the long term. This included creating an investment plan and mapping financial flows and potential co-financing.

Communication Plan

Communication plan to increase visibility of the ecosystem and the cluster and ensure stakeholder engagement (target group identification, strategic messaging, communication channels).

2.2 Mixed-Methods Approach

A mixed-methods approach was used for this study, combining quantitative and qualitative research methods. The methodology focused on both foresight and intensive stakeholder interaction and consisted of the following key components:

Foresight – Vision, Mission and Strategy

The foresight study formed the core of the methodological approach. This future exploration aimed to develop a shared long-term perspective on critical maritime infrastructure (CMI) in the Belgian North Sea, with a time horizon to 2050 and a focus on the next 5 years.

The study began with an in-depth foresight analysis. Relevant societal, technological, and geopolitical trends, drivers, and uncertainties impacting maritime safety were mapped. The existing maritime infrastructure was analysed for vulnerabilities and economic value. Based on this, four plausible scenarios were developed, forming the foundation for formulating robust strategic choices (see section 3.3).

Ecosystem interaction: stakeholder engagement and co-creation

A second major pillar of the methodology was intensive interaction with the broader ecosystem, both to gather input and build support.

Interaction took place at several levels:

Mapping and analysis of the ecosystem

An inventory was made of the companies, knowledge institutions, and actors active in CMI protection, as well as the relevant technological themes. Their positions in the value chain (energy, communication, ports) were analysed.

In-depth interviews

Based on the ecosystem analysis, semi-structured interviews were conducted with experts from various domains (technology providers, users, integrators, research institutions). These interviews aimed to gain better insight into the actors (companies, knowledge institutions, integrators, etc.) involved in CMI protection R&D and innovation, and to discuss their challenges, priorities, and expectations regarding a future ecosystem.

The interviewed experts represented various links in the value chain of CMI protection across the three identified domains: energy, communication, and ports.

The in-depth interviews focused on the following themes:

- Assessment of CMI security and threats;
- Innovation in technology and solutions;
- Market potential for CMI protection;
- Insight into the ecosystem and value chain;
- Key factors for value creation within a CMI ecosystem;
- Governance and management of the ecosystem;
- Interest in and willingness to engage in a CMI ecosystem.



List of stakeholders involved in the study

The results of these in-depth interviews can be found in section 5.3

Individual questionnaire

In addition to the interviews, an individual questionnaire was distributed to collect expectations regarding the ecosystem and especially the priorities to be set.

The insights gained from these interviews were an important input for further developing the feasibility study, in which we map out the opportunities and preconditions for a sustainable ecosystem around CMI protection. These conversations also helped build support among participating companies and knowledge institutions regarding a future ecosystem.

Advisory group

To enhance the quality and relevance of the feasibility study, an advisory group was established consisting of representatives from industry and relevant stakeholders. This group served as a sounding board and critical reflection forum throughout the study process.

The advisory group met monthly during the study period. During these meetings, the research progress was discussed, and preliminary insights were shared. Members of the advisory group provided valuable input, reflections, and feedback that contributed to the deepening of analyses and the enrichment of results.

Throughout the process, the advisory group members were actively informed about the project's progress. Their expertise and involvement contributed to the quality of the final outcome and ensured the study was closely aligned with the needs and expectations of the industry.

The advisory group consisted of: e-BO-Enterprises; Port of Antwerp-Bruges; Exail; Parkwind; Thales group; Elia; Sabca; Damen; Fluxys; BICS; and the Belgian Navy.

Structural consultation

There were several steering groups with DIRS management. Throughout the process, collaboration took place with partners such as Sirris, DIRS Management, and INNOCOM, who provided substantive expertise and procedural support. This collaboration ensured continuous alignment and quality assurance.

CONCLUSION

The study was conducted through five work packages, focusing on vision and strategy, governance, ecosystem development, financial structuring, and communication.

At its core, the approach combined quantitative and qualitative methods, built around two pillars: foresight and intensive stakeholder interaction. The foresight analysis formed the basis for long-term strategies toward 2050, with a particular focus on the next 3 to 5 years. Four future scenarios were developed based on trends, risks, and system vulnerabilities.

The broader ecosystem was mapped through in-depth interviews, a questionnaire, and regular consultations with stakeholders, including technology providers, users, integrators, and research institutions. These engagements provided key insights into market opportunities, technological priorities, governance, and willingness to collaborate.

An advisory group of industry representatives ensured ongoing quality control, critical reflection, and alignment with sector needs. Collaboration with expert partners further reinforced the process and content. This methodological approach not only generated valuable insights but also fostered strong engagement and support for developing a sustainable, innovative ecosystem for CMI protection.



3. Ecosystem Mission and Vision

Introduction

A clear and sharp mission and vision is fundamental to set up a future-proof strategy to build the CMI ecosystem. A compelling mission with a clear vision is required to build a strategy for the organisation with a timeframe of 10 years, which is further worked out in strategic priorities with a time window of 5 years.

3.1 Mission

Enabling the protection of maritime infrastructure through innovation and collaboration

Mission Statement

By fostering collaborative innovation, knowledge sharing, and market valorisation, the CMIP ecosystem creates immediate economic value and societal impact while strengthening the resilience and security of our critical maritime infrastructure.

The CMIP innovation ecosystem is dedicated to enhancing the protection and resilience of critical maritime infrastructure, including offshore energy assets, communication infrastructure and ports, against hybrid and emerging threats.

3.2 Vision

Build a forward-looking, internationally connected, and resilient innovation ecosystem that positions Belgium as an international leader in the protection of critical maritime infrastructure.

The ecosystem will serve as a catalyst for economic growth, strategic partnerships, and the development of world-class capabilities, supporting the long-term security, competitiveness, and sustainability of the Belgian maritime sector.

This can be achieved by:

- Connecting the economic ecosystem: stimulating dual-use innovation, facilitating cooperation and synergies between companies, knowledge institutions, government and, where relevant, citizens and encouraging cross-sector collaboration;
- Accelerating the development and adoption of emerging technologies and enabling the deployment of scalable and interoperable solutions that protect strategic maritime assets;
- Supporting international cooperation and market development, with a focus on 'Made in Europe.'

3.3 Strategic Foresight

In the context of the feasibility study, a foresight study was conducted to find out which technologies - under which conditions - show significant economic and strategic market potential and how these technologies fit within the uncertainties of the future, and which ones can be considered future-proof.

Scope

1. **Geographic**: The focus is, in the first instance, on the Belgian North Sea and the Scheld estuary and, in the second instance, on Europe. Global trends and developments are taken into account where they have a direct impact on the safety and security of the Belgian North Sea and ports. In addition, the transatlantic export potential of the developed technologies is considered.

2. **Time-bound**: The time horizon is 2050. The purpose of this distant future projection is to provide a long-term perspective in which technologies currently under development are given sufficient time to reach their full potential. This allows a wide range of current innovations and emerging technologies to be included in the analysis.

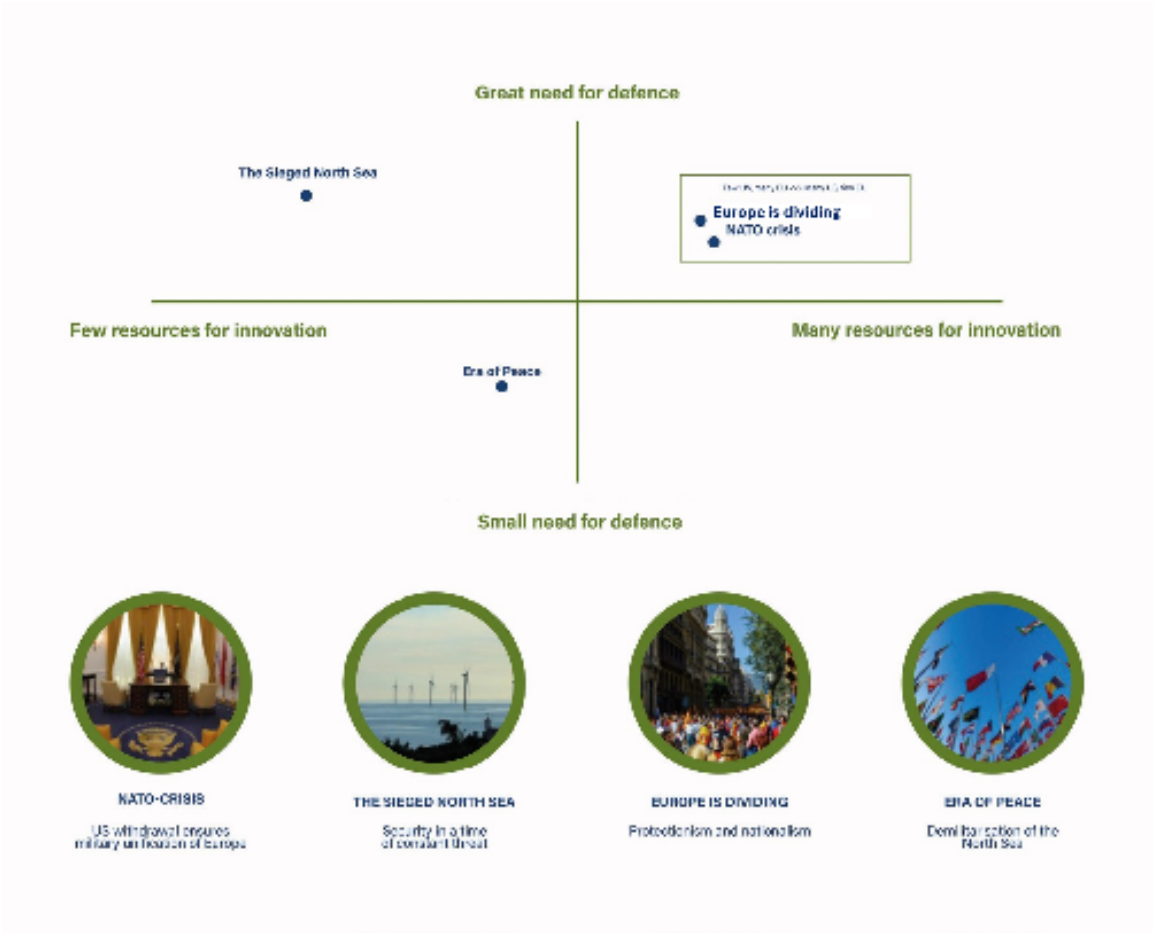
3. **Technological**: The scope includes innovations related to security under, on and above the water, and in three sectors: energy, communications and ports. The focus is preferably on technologies developed by Belgian companies so as to encourage the involvement of national players and maximise their potential in the Belgian North Sea and ports.

Scenarios towards 2050

The foresight study analyses certain possible but less likely futures. These are studied not because they are expected, but because they offer valuable insights across the spectrum of possible futures.

Based on an in-depth research on existing and emerging trends and drivers, insights were gained into the structural changes and forces shaping the future.

From an initial long list of 16+ scenarios, 4 'extreme' ones were selected using the axis 'Few or Plenty of resources for innovation' and 'High or Low need for Defence'.



Scenario 1 - NATO-crisis: US withdrawal ensures military unification of Europe

The US is withdrawing from NATO and forcing European countries to build their own defence capabilities. Together with the presence of external threats, such as aggressive geopolitical actors, the EU is forced into closer military cooperation and the creation of a European command.

Consequences:

- Belgium is investing heavily in joint and centralised European command and maritime defence cooperation;
- This also offers a partial solution to the current problem of fragmented security powers in Belgium, and ensures that larger orders can be placed allowing economies of scale to be realised.

Scenario 2 - Europe is dividing: Protectionism and nationalism

The EU is slowly disintegrating through a return to protectionism and national interests, leading to reduced defence cooperation. The United States sees this evolution as an opportunity to further expand its global influence.

Consequences:

- Belgium must invest in maritime defence itself without European support, leading to limited capabilities and increased vulnerability;
- However, it can still call on the overarching support from the United States.

Scenario 3 - The Sieged North Sea: Security in a time of constant threat

Critical infrastructure in the Belgian North Sea and ports is being targeted by a sustained wave of attacks. The attackers remain below the threshold of open war, but the impact is devastating: economic disruption, increased political pressure and a defence sector forced to deploy all its resources for immediate response. Belgium finds itself in a vicious circle of crisis management without a vision for the future.

Consequences:

- Although the budget for the Navy is increasing, this goes entirely to crisis management, leaving no room for public investment in innovation;
- On top of that, it becomes all the more important to build a robust business case that also creates sufficient societal value creates;
- Cooperation with private actors and allies becomes crucial to ensure security.

Scenario 4 - Era of Peace: Demilitarisation of the North Sea

A period of unprecedented diplomatic stability is dawning, with military spending declines worldwide. Belgium and Europe focus on civilian maritime cooperation.

Consequences:

Navy and defence are given a purely supporting role (e.g. humanitarian missions), and focus shifts to crisis management and disaster relief.

Strategic Foresight Recommendations

Based on the scenario analysis and modelling for an innovation ecosystem around maritime security technologies, 6 strategic recommendations have been formulated.

These recommendations form the foundation for the creation of an innovation cluster around maritime security and defence technologies and have been integrated in the final recommendations for the establishment of the ecosystem (see chapter 11). They ensure technological resilience, societal legitimacy and economic scalability in a variety of future scenarios.

1. Stimulate dual-use innovation with private players
2. Further develop the niche expertise of Flanders in drones and capitalize on its export potential
3. Use the development of a digital twin of the Belgian North Sea as a moonshot project
4. Invest strategically in the development of repair drones to create a first-mover advantage
5. Establish a task force focusing on interoperability and European standardisation
6. Anchor ethics and societal relevance

The final recommendations are discussed in more detail in Chapter 11. Further information on relevant strategic actions and more specifically the formulation of key actions can be found in Annex 3.

4. Market

Introduction

This chapter provides a comprehensive assessment of the market potential for Critical Maritime Infrastructure Protection (CMIP). It aims to validate the economic feasibility of establishing an innovation ecosystem dedicated to safeguarding vital maritime assets, with a focus on surveillance, detection and response, communication, data exchange, and repair technologies. The analysis draws on global and European market data, the recent foresight study by Ortelius and sectoral trends to identify growth opportunities for our CMIP ecosystem companies.

4.1 Market Drivers and Macro Trends

The blue economy is poised for robust growth, with global annual value projected to reach €3 trillion by 2030, representing about 5% of global GDP. Key sectors include offshore renewable energy, aquaculture, maritime transport, and data infrastructure. Europe's blue economy is growing strongly, particularly in shipping, offshore energy and emerging sectors such as marine biotech and blue digitalisation.

Offshore wind is the fastest-growing segment, with Europe's market expected to grow at a compound annual growth rate (CAGR) of 8–10% over the next decade. Offshore wind capital expenditure and spatial demand for offshore energy infrastructure is set to increase nine-fold. This expansion increases the density and strategic importance of maritime assets, heightening the need for advanced critical infrastructure protection solutions.

Digitalisation is reshaping maritime operations, with the maritime digitisation market projected to reach $298–423 billion by 2028–2031 (CAGR of 0.7%). The adoption of digital twins, IoT, AI, and autonomous systems is accelerating, enabling real-time monitoring, predictive maintenance, and enhanced situational awareness. These technologies are foundational for next-generation CMIP.

Recent incidents have catalysed regulatory action and investment in defence and maritime security. The foresight study by Ortelius highlights scenarios of increased hybrid threats and the strategic vulnerability of North Sea infrastructure, emphasising the urgency for robust, integrated critical infrastructure protection frameworks.

4.2 Market Dynamics and Public Investment

The market for Critical Maritime Infrastructure Protection (CMIP) is experiencing clear growth.

Globally, demand for maritime security technologies is increasing, driven by geopolitical tensions and the rapid development of the blue economy. At the same time, governments are significantly raising their defence budgets, with a growing share allocated to the maritime domain.

These developments create substantial opportunities for companies active in CMI protection. A detailed analysis of market growth, technology adoption, and public investment trends is provided in annex A4.

The conclusions of a top-down calculating of public spending on maritime security technologies are:

- At current % of GDP, public spending on R&D and purchases for the Navy is estimated at €136 billion in 2025 and €225 billion in 2050 for European NATO countries, US and APAC (excluding China and India);
- If NATO countries were to spent 4%, this rises to €297 billion in 2050;
- Of this, the US remains the largest public investor;
- With varying input variables for the four scenarios, spending ranges between €115-€322 billion in 2050.

4.3 Security Value (based on technology model)

A bottum-up calculation based on the critical maritime infrastructure present and the estimated use of technologies to secure it results in an estimated maximum total security value of technologies to secure infrastructure.

Technology domains

In the context of the study, 5 technology domains were selected as being most relevant for CMI protection.



Fixed Surveillance

- Fixed systems designed primarily to monitor or detect activity within a specific area, through passive or active detection. These systems lack autonomous response capabilities, without performing data analysis functions and communication relay.
- Examples: Cameras, radar installations, sonar arrays, hydrophones, sensors on the seabed...

Drones

- Mobile robotic systems (air-, surface-, underwater- or land-based) that autonomously or semi-autonomously navigate physical environments to collect data, conduct monitoring, or perform localised tasks. Their primary function is based on mobility rather than fixed installations.
- Examples: UAVs, USVs, AUVs, four-legged robots, inspection drones...

Automated systems > Robotics

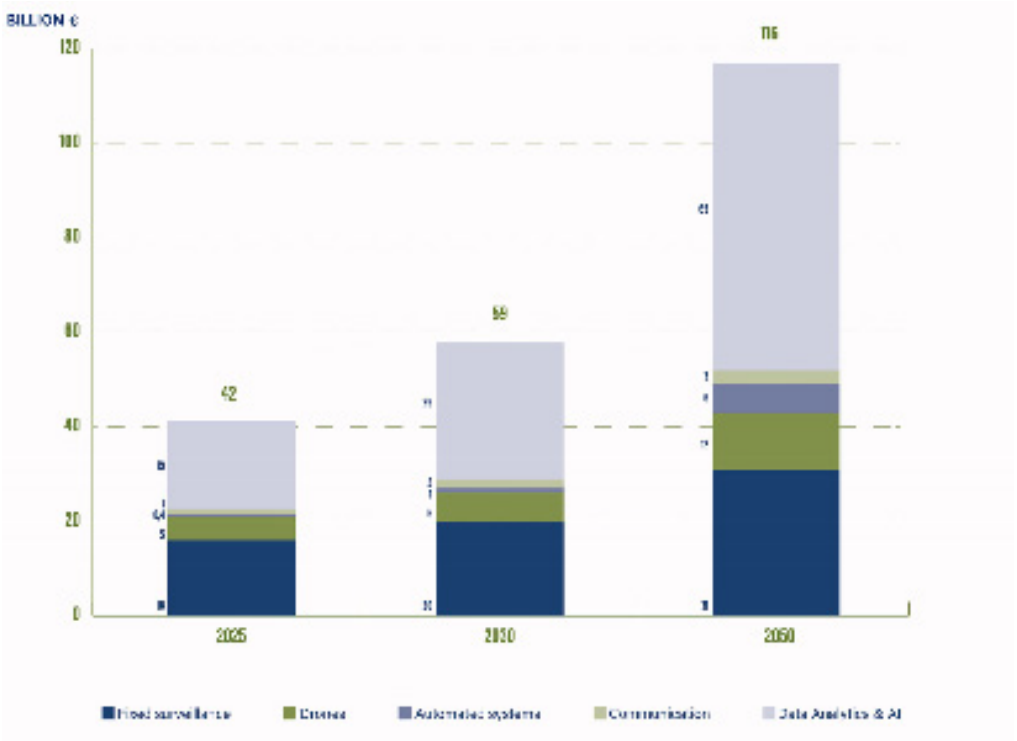
- Autonomous or semi-autonomous physical systems that are embedded, tethered or integrated into larger infrastructures, capable of executing pre-programmed or AI-controlled actions in response to environmental stimuli. These systems do not rely on mobility and are not primarily focused on sensing, communication or data analysis.
- Examples: Robotic arms, firefighting systems, pressure control valves, anti-intrusion locks...

Communications

- Systems to ensure the transmission, routing or integrity of data, commands or alerts between physical and digital components. These systems do not perform detection, analysis or physical actions themselves.
- Examples: SCADA networks, 5G nodes, maritime radio links, repeaters on submarine cables...

Data analytics & AI

- Systems who analyse and interpret collected data or make predictions—such as pattern recognition, threat classification, behavioural modelling, and operational optimisation—without collecting raw data or performing physical actions themselves.
- Examples: Software for predictive maintenance, models for anomaly detection, AI systems for threat analysis, dashboards for behavioural prediction...



Data Analytics & AI represent the biggest growth opportunities.

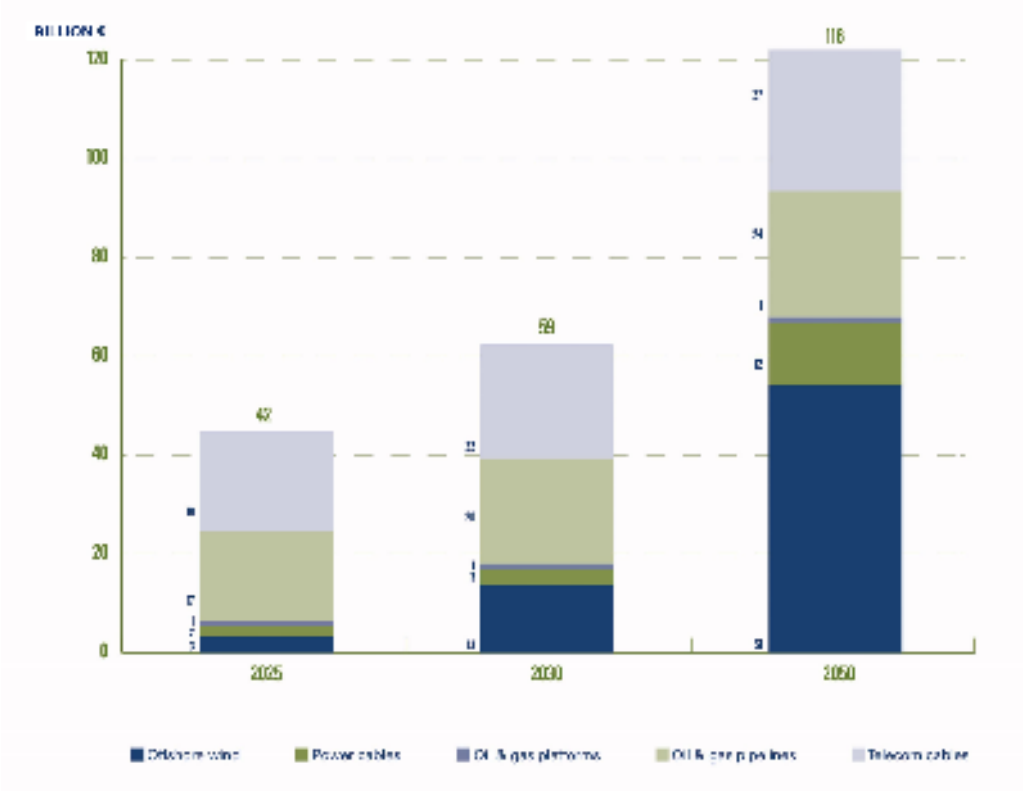
The security value has been calculated based on the amount of infrastructure present multiplied by the effective range of the technology and multiplied by the CAPEX investment for the implementation of the technology.

This has been calculated for the period 2025, 2030 and 2050, resulting in the theoretical maximum of the total security assets needed, expressed as the investment volume that would be required to fully equip all critical maritime infrastructure in a given year with the relevant technologies.

For the 3 core markets (EU, US, APAC) this results in an estimated market value of €42 billion, growing to about €60 billion in 2030 and doubling to €116 billion in 2050. The biggest growth will come from **Europe**, driven by the uptake of offshore wind and power cables.

The biggest potential comes from Data analytics and AI, where a tripling of the potential maximum of the security value is expected, accounting for about 50% of the market. Fixed surveillance has a more modest growth but expectation is that by 2050 these represent about €30 billion (or 27% of the market).

The drone technology security value is growing healthily but is much smaller in volume (€12 billion in 2050) due to the relatively low CAPEX per drone unit and extended range of drone units. Communications and Automated systems are remaining relatively small markets.



The growth of offshore wind is the biggest driver for growth in the CMIP market.

CONCLUSION

The market for CMIP is set for sustained, double-digit growth, underpinned by the expansion of the blue economy, the increase of public defence spending, offshore renewable energy, and maritime digitalisation. The sector's value is projected to nearly triple by 2050, with Europe at the forefront of both demand and innovation. The opportunities related to the growth of offshore wind represent a potential market for CMIP in Belgium alone of €560M in 2050, up from €90M in 2025.

Technology companies have significant opportunities in domains such as autonomous systems, AI, digital twins, and secure communications. Early engagement in standardisation and dual-use innovation will be key to capturing market share.

Leaving out the US, the main growth market for maritime defence is Europe, with key countries yet to be defined.

5. Technology mapping, stakeholder landscape and the voice of the stakeholders

Introduction

Protecting Critical Maritime Infrastructure (CMI) requires more than advanced technology alone—it demands a robust and coordinated ecosystem of stakeholders. This chapter provides a comprehensive mapping of the technological landscape and the stakeholder ecosystem essential for advancing Critical Maritime Infrastructure Protection (CMIP).

By systematically cataloguing the five core technology domains—including fixed surveillance, drones, automated systems and robotics, communications and connectivity, data analytics, and AI—we highlight the breadth and depth of Belgium's technological capabilities and innovation assets.

We identified key players such as technology providers, research institutions, and innovation hubs, and demonstrate how their expertise and collaboration can be leveraged to tackle CMIP challenges. Furthermore, through targeted interviews and survey responses, the voices of stakeholders from defence, industry, research, and government confirm and enrich our understanding of the value drivers, priorities, and structural conditions necessary for establishing an effective Research, Technology, and Innovation (RTI) ecosystem. This chapter lays a solid foundation for building a dynamic CMIP ES and identifies strategic opportunities for ecosystem partners.

5.1 Technology and stakeholder mapping

Following the introduction of the five technology domains in chapter 4, the table on the next pages details for each domain a number of subdomains. It also summarises the general key technologies applied per subdomain and the primary function of each subdomain in CMI protection.

This table lists examples of Belgium-based technology and solution providers per subdomain. It is important to emphasise that, in many cases, this overview only captures a subset of their activities. Each company is listed under a maximum of two subdomains, even though many are active in more subdomains. This overview is by no means exhaustive but provides an initial basis for future outreach and mobilisation in the context of the CMI protection ecosystem. This highlights how vibrant the ecosystem is across all these domains.

Fixed Surveillance

Subsea Surveillance Systems

Definition	Permanently or semi-permanently deployed systems on the seabed or in the water column designed to detect, track, and classify underwater objects or activities.
Key technologies	Active sonar (IDS/DDS), passive sonar (LOFAR), distributed acoustic sensing (DAS), magnetic anomaly detectors (MAD), seabed sensors, environmental monitoring sensors
Primary function and application	Monitoring critical subsea infrastructure, detecting underwater threats (divers, AUVs), environmental data collection.
Examples of Belgium-based technology and solution providers	Active Drone Security Solutions, Advionics, Automatic Systems, Belgian Advanced Technology Systems (BATS), Centum Technologies & Solutions, Helicus, Hexagon-Luciad, IR&D Infrared Research and Development, Lambda-X, Marlinks, OIP Land Systems, OIP Sensor Systems, OIP Space Instruments, Redwire Space, Safran, Securitas, Senhive, Spacebel, Stentor, Teledyne, Unacis, Verhaert, VITO, Xenics / Exosens

Surface & Air Surveillance Systems

Definition	Fixed systems positioned on land, on offshore installations or satellite platforms to monitor surface vessels and airborne objects, providing situational awareness above the waterline.
Key technologies	Coastal radar installations, fixed cameras incl. 360°, satellite monitoring, drone detection sensors, AIS-based systems
Primary function and application	Detecting and tracking surface vessels and airborne objects, providing visual monitoring and situational awareness around infrastructure
Examples of Belgium-based technology and solution providers	24Sea, CMRE, Gardec, Mirion, Patria

Drones

Unmanned Aerial Vehicles (UAVs)

Definition	Remotely or autonomously controlled aircraft operating without a pilot.
Key technologies	Fixed-wing (speed, range, large payloads), rotary-wing (VTOL, hovering, precise data), unmanned airships (long endurance, command centres), para-wing (lightweight, versatile), fluttering (high mobility, communication relays)
Primary function and application	ISR (Intelligence, Surveillance and Reconnaisance), Aerial surveillance, reconnaissance, marine patrol, rescue, pollution forensics, logistics, military operations.
Examples of Belgium-based technology and solution providers	Citymesh, DroneMatrix, Droprise, Flying-Cam, Helicus, Lockheed Martin, RTX, Sabca, Safran, Sky-Hero, SkeyDrone, Sol.One, Space Applications Services, Unifly, Xenics / Exosens, ZSE Technology

Unmanned Surface Vehicles (USVs)

Definition	Autonomous or semi-autonomous vessels operating at or near the sea surface without onboard operators.
Key technologies	Navigation (GNSS, INS, autopilot, collision avoidance, path planning, AI/ML), sensors (radar, LiDAR, optical cameras, sonar, environmental sensors, AIS), communication, propulsion and energy, vehicle design and materials
Primary function and application	ISR, Intelligence gathering, mine detection/neutralisation, anti-submarine warfare, resupply, direct engagement, data transmission.
Examples of Belgium-based technology and solution providers	Exail Robotics Belgium, GEOxyz, MAHI, Sky-Hero, dotOcean

Autonomous Underwater Vehicles (AUVs)

Definition	Unmanned underwater robots accomplishing missions through autonomous control.
Key technologies	Navigation (INS, DVL, acoustic positioning systems, sensor fusion, SLAM), sensors (sonar systems, optical cameras, LIDAR, environmental sensors, magnetometers), communication (high complexity), propulsion and design
Primary function and application	Seafloor mapping, infrastructure integrity checks, underwater threat engagement, environmental data collection, underwater search.
Examples of Belgium-based technology and solution providers	CMRE, Exail Robotics Belgium, GEOxyz, Naval Group, Thales, VLIZ

Counter-UAV Systems

Definition	Technological solutions designed to detect, track, identify, and neutralise unauthorised or hostile unmanned aerial vehicles (UAVs or “drones”).
Key technologies	Detection (RF, radar, acoustic, optical, IR), tracking (automated PTZ cameras, radar, RF, sensor fusion), identification (RF fingerprinting, video analytics/AI, drone databases), neutralisation (RF jammers, GPS spoofing, net capture, high-energy lasers, kinetic interceptors, cyber takeover)
Primary function and application	Protecting shipping lanes, terminals, offshore and coastal energy and communications platforms from aerial surveillance and attacks within a secure perimeter.
Examples of Belgium-based technology and solution providers	Active Drone Security Solutions, Belgian Advanced Technology Systems (BATS), Senhive, ZSE Technology

Automated systems & Robotics

Onboard Control & Operational Systems

Definition	Automated systems integrated into vessels or fixed maritime installations to manage and optimise core operational functions.
Key technologies	Automated autopilot, dynamic positioning, integrated bridge systems, engine & machinery control, cargo handling, ballast water treatment
Primary function and application	Enhances efficiency, safety, and performance; reduces manual intervention; optimises operational reliability and resilience.
Examples of Belgium-based technology and solution providers	Anglo Belgian Corporation (ABC), ACB, Any-Shape, Antwerp Maritime Academy, Barco, Centum Technologies & Solutions, De Meyer, DEME, EDR Antwerp Shipyard, ELCOS, Flanders Ship Repair, Gardec, Grimonprez, GROUPEMECA: Vanhulen, Honeywell, ILIAS Solutions, Jan de Nul, Jean Del'Cour (JD'C), LGM Group, Mockel Precision, MOL, Montana Aerospace, MULTI.engineering, Mustad, Naval Group, New Lachaussée, OIP Land Systems, OneBonsai, Revimaxx, RWE, Sabca, Sabena, ScioTeq, Seafar, Simtech, Sonaca, Space Applications Services, Telerex, Ugent, VIRO, VKI, Vlassenroot

Integrated Safety & Security Systems

Definition	Automated systems designed to monitor, detect, and respond to safety hazards and security breaches within maritime infrastructure.
Key technologies	Fire detection & suppression, intrusion detection, emergency response, access control, alarm response, screening technology
Primary function and application	Provides real-time alerts and automated countermeasures; enhances physical security and safety from internal threats
Examples of Belgium-based technology and solution providers	Automatic Systems, Droprise, FN Herstal, John Cockerill, Mirion, Pitagone, Securitas

Communication & Connectivity

Operational Technology (OT) Networks

Definition	Networks and systems controlling physical processes and devices within maritime operations.
Key technologies	SCADA systems, propulsion & machinery management, navigation systems (GPS, ECDIS, RADAR), bridge systems, HVAC, fire detection networks
Primary function and application	Direct control of vessel/port or other business operations; critical for cyber-physical security.
Examples of Belgium-based technology and solution providers	Cisco, EMDYN, Elia, ILIAS Solutions, e-BO Enterprises

Information Technology (IT) Networks

Definition	Networks and systems for data processing, information management, and administrative functions.
Key technologies	Administrative & crew welfare systems, cargo control systems, environmental control systems, access control & screening systems, shore-to-ship data exchange
Primary function and application	Supports administrative, logistical, and crew functions; facilitates data exchange
Examples of Belgium-based technology and solution providers	Approach Cyber, Axians, Cisco, Cronos, DNV-Cyber security maritiem, imec, Inetum, Lockheed Martin, Made, Médiane Benelux, Prodata, Rhea, Sirris, Sopra Steria, Toreon

External Communication Systems

Definition	Infrastructure and protocols enabling communication between maritime assets and external entities.
Key technologies	Satellite communication (Satcom), maritime radio links (GMDSS), 5G nodes, submarine cable repeaters, AIS, GNSS/GPS
Primary function and application	Ensures data transmission, command relay, and alert dissemination across the maritime domain.
Examples of Belgium-based technology and solution providers	Citymesh, e-BO Enterprises, Nemand, Nokia Defence International, Patria, Skeydrone, ST Engineering, Thales, Unifly

Data analytics & AI

Threat Detection & Anomaly Identification

Definition	AI/ML models identifying malicious activities, deviations, or unusual patterns in maritime data.
Key technologies	Machine learning, unsupervised learning, deep learning, reinforcement learning
Primary function and application	Real-time intrusion detection, identification of navigation anomalies, unauthorised access, and irregular data transmissions.
Examples of Belgium-based technology and solution providers	Approach Cyber, Dronematrix, EMDYN, Inetum, Médiane Benelux, Prodata Systems, Rhea, Sol.One, Sopra Steria, The Cronos Group, Toreon

Predictive Analytics & Risk Assessment

Definition	AI-driven systems analysing data to forecast threats, predict failures, assess risks, and optimise operations.
Key technologies	Deep learning (CNNs, RNNs), natural language processing (NLP), graph-based AI
Primary function and application	Predictive maintenance, maritime threat prediction, cyber risk assessment for autonomous vessels, cyberattack forecasting.
Examples of Belgium-based technology and solution providers	24Sea, Antwerp Maritime Academy, Axians, DNV-Cyber security maritiem, iCare, LGM group, Marlinks, MULTI.engineering, Sirris, Viro, VITO

Data Integration & Situational Awareness

Definition	AI/ML platforms converging disparate data inputs for unified, actionable situational awareness.
Key technologies	AI/ML platforms, federated learning, blockchain-enhanced AI
Primary function and application	Synthesising data from multiple sources, secure data exchange, privacy-preserving learning, enhanced overall maritime domain awareness.
Examples of Belgium-based technology and solution providers	Barco, dotOcean, Hexagon-Luciad, IDLab UGent, imec, MAHI, ML6, Nokia Defence International, Officers on Watch, One.Bonsai, OIP Space Instruments, ScioTeq, Seafar, Spacebel, Verhaert, VLIZ

5.2 Our strong foundation in science, technology research and innovation

Belgium boasts world-class universities, strategic research centres, and innovation hubs that provide the knowledge, expertise, and talent needed to place us at the forefront of maritime innovation, with a particular focus on solutions for Critical Maritime Infrastructure Protection (CMIP).

These organisations have long focused on technology transfer, company creation, and the commercial valorisation of their research outputs. However, they often lack the resources to fully translate their research into market-ready products and services.

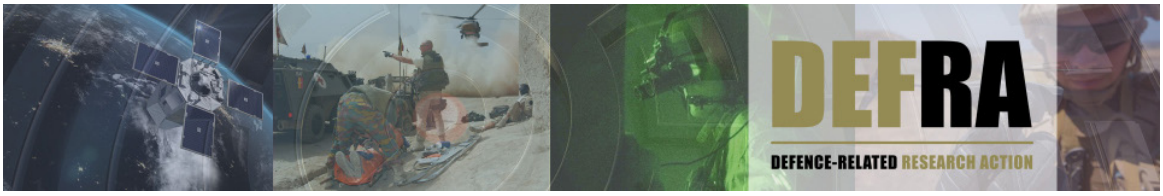
For defence and security innovation, it is crucial to leverage this pool of excellence, as it offers our ecosystem companies a significant competitive advantage and positions Belgium as a leader in niche CMIP applications.

Here are some examples of how universities and RTOs contribute to the CMIP domain:

IMEC:

DEFRA (Defence Related Research Action), launched in 2021, brings together universities, strategic research organisations, and companies to address challenges proposed by defence communities. The increasing success of DEFRA calls highlights the strong commitment of the research and innovation community to defence.

Several DEFRA projects focus directly on CMIP. For example, imec is involved in two DEFRA 2024 projects, including Aqua-Mesh, which investigates improved underwater communication between sensors, weapon systems, and data systems. Running from December 2024 to March 2028, Aqua-Mesh leverages imec/IDLab's expertise in communication networks to build a competence centre for underwater communication, with the potential creation of a start-up as an outcome.



Ghent University and Howest Cyber 3 Lab:

Both institutions collaborate on secure cloud environments, sovereign cloud infrastructures, and data spaces. These core technologies underpin next-generation situational awareness platforms that use AI to accelerate detection, support planning and decision-making, facilitate reporting, and continuously enhance CMIP processes.



UGent IDLab and Howest work together in the domain of Cyber OT, relevant for CMIP

Flanders Marine Institute:

Flanders Marine Institute (VLIZ) stands for interdisciplinary research of the ocean, seas, coast, and estuaries. VLIZ has built up a strong expertise in underwater drones, digital twin models of the North Sea, and data fusion. The underwater sound library is one example of a unique VLIZ asset.

Flanders is investing in the development of an underwater sound library for the North Sea. With these funds, VLIZ aims to achieve automatic recognition of natural and human noise sources in the sea. Such knowledge and tools are essential for offshore security and for numerous AI-based research initiatives. Access to these know-how and assets is key for our future CMIP systems.



VLIZ is creating an underwater sound library, a key asset for CMIP

FLANDERS MAKE:
Flanders Make is one of our strategic research centres in the domain of industry 4.0 and industry 5.0 that performs high-tech research in manufacturing with and to the benefit of companies. Its mission is to bring disruptive innovation to industry so as to make it stronger and more competitive.

Flanders Make contributes to product and manufacturing innovation for many industries such as automotive, maritime, industrial machines and factories. Their research covers areas such as computer vision for quality control, software for industrial machines and automation and electrification of transportation means.

Belgium possesses outstanding scientific resources, innovation potential, and world-leading expertise that will play a crucial role in the future of CMIP systems. The ecosystem should unite scientific and research communities with start-ups, innovative SMEs, and corporates to strengthen knowledge, provide access to top expertise and talent, and translate the best research outcomes into competitive market products that significantly enhance the protection of critical infrastructure.

The ecosystem's role is to:

1. Maintain an overview and monitor existing projects for potential application in future CMIP innovations or start-up opportunities;
2. Initiate new applied research and innovation projects addressing CMIP challenges;
3. Connect the various stakeholders to foster collaboration and knowledge exchange.

5.3 Stakeholder perspectives on an RTI ecosystem

During the depth interviews, respondents listed various expectations regarding the proposed Research, Technology, and Innovation (RTI) ecosystem:

A. STRENGTHEN COLLABORATION AND NETWORKING

The ecosystem is seen as essential for bringing people and competencies together. There is a need for a formal network where contacts between defence, private sector and RTOs are facilitated in a structured manner with a clear mission-based focus. To accelerate tangible results, the ecosystem needs to apply an open approach, mobilise complementary technology competences and partners and apply a targeted "coalition of the willing" approach.

It should focus on bringing the right parties together and engage with **champions** to take the lead and bring other companies along. Champions are companies with a track record in collaborative innovation, a unique position in the value chain and preferably a historical relationship of trust with defence.

The ecosystem should help with consortium formation for projects and tenders and become a breeding ground for joint ventures and partnerships with a scaling up agenda. Participants will build trust amongst themselves and with defence and other security actors through regular but action-focused interaction, joint collaboration projects, tangible innovation results and successes.

B. FACILITATE SECURE AND EFFICIENT DATA ACCESS AND SHARING

Improving situational awareness in the protection of maritime infrastructure depends largely on ready access to a variety of historical, dynamic and real-time subsea, surface-level, aerial and space-based sensor data, smart data fusion, AI-supported analysis, interpretation and visualisation for decision-making. Data are often maintained in silos with restricted data access and sharing for technical, commercial and security reasons.

The ecosystem can assist in the identification and removal of some of these barriers in data access and in data sharing, aggregation and valorisation of data from different sources. Secure data exchange between different actors (military and non-military) is crucial. This requires a data-centric security approach with practical data sharing frameworks, interoperability standards, access to infrastructure for large-scale data processing (geo intelligence hub/data centre)

C. DEVELOP WELL-ALIGNED DEMAND-DRIVEN TECHNOLOGY ROADMAP

The ecosystem should coordinate the development of a detailed and dynamic innovation roadmap defined on basis of the defence and public sector (federal, regional) priorities, the Belgian private sector strengths and capabilities and the upscaling and economic valorisation potential. The support of the government, i.e. defence, in defining requirements, streamlining processes, and providing support in the innovation roadmap and priorities is a critical expectation.

Next to the government as potential end customer for security solutions, many use cases will have CMI operators and owners as investing customer. Their structural representation in the ecosystem and the development of the innovation roadmap is essential. A clear definition and involvement of the end-customer in every innovation trajectory is essential to derisk private sector investments and maximise return on investment.

D. TRANSPARENT, LIGHT-WEIGHT AND FAST-TRACK INNOVATION FUNDING PROCEDURE

The ecosystem should be focused on concrete projects, well-defined challenges and tangible short-term results. Processes and structure should allow for speed and agility, light and lean procedures with short lead times, applying "fail fast, learn fast" principles.

The ecosystem must facilitate the development and adoption of governmental funding mechanisms with shorter lead-time, reduced administrative burden and higher funding rates than the current portfolio of innovation funding instruments (e.g. VLAIO and DEFRA). Transparency is important, especially with regard to funding calls, procurement procedures and opportunities.

There is a clear need to create innovative financing instruments and co-funding for projects that close the gap between TRL 5-9 and support industrialisation, commercialisation, market access (national and international) and business development. Instruments such as cascade funding (indirect funding mechanisms) should assist to facilitate financial support for start-ups and SMEs through the deployment of lighter procedures and faster decision-making.

E. STRENGTHEN BELGIUM'S INDUSTRY INNOVATION CAPACITY WITH A PARTICULAR FOCUS ON SMEs

A key role of the ecosystem is to boost Belgium's industrial innovation capacity by stimulating local involvement and ensuring that Belgian industry benefits from defence investments. While Belgium does not host major defence platform manufacturers or prime contractors, it has a diverse and capable industrial base with strong potential to act as suppliers to these platforms.

The ecosystem must create opportunities for Belgian companies to engage with the defence sector, familiarise themselves with its procedures, requirements, and working culture, and build trusted relationships with defence and CMIP stakeholders. This could include organising workshops and training programmes that help companies understand defence procurement processes and security requirements, as well as hosting networking events and matchmaking sessions to connect Belgian suppliers with prime contractors and end-users within the defence ecosystem.

Furthermore, the ecosystem is expected to consolidate Belgian technological expertise, promote dual-use applications, support SMEs in gaining access to both national and international markets, and raise awareness and proactive engagement regarding the security of Critical Maritime Infrastructure (CMI).

F. SCALING AND INTERNATIONALISATION

The Belgian market is too small, so internationalisation is a very important aspect for the ecosystem. The goal is to promote Belgian expertise globally. The ecosystem should support market valorisation and scaling of homegrown innovation. This requires a concerted approach with governmental agencies (i.e. FIT, AWEX, Hub Brussels) to facilitate participation in trade missions, international conferences and expos but also structural linkages with RTI clusters in other European and trans-Atlantic countries. Exploiting market potential, particularly dual-use and international growth, is an important driver.

Funding for start-ups and SMEs should not be restricted to collaborative innovation trajectories but should also include support for market and business development.

G. TESTING GROUNDS AND LIVING LAB

Many respondents emphasised the need for an available test area with low regulations to perform early-stage real world tests in a realistic environment and access to feedback from the end customers (operators, marine, etc.). Ports, such as Port of Antwerp-Bruges and North Sea Port, position themselves as testbeds or living labs where technologies can be tested and scaled up from laboratory models to a higher level. The ecosystem can create an environment for experimentation and testing the interoperability of systems.

Access to military personnel for realistic operational contexts and test platforms is crucial for the development and validation of dual-use technology.

H. NEUTRAL AND TRANSPARENT ECOSYSTEM MANAGEMENT ORGANISATION

Considering the competitive aspects in collaborative innovation and valorisation, the ecosystem manager needs to have a neutral position and have expertise in managing obvious conflicts of interest and divergent priorities of its members. This requires transparent and inclusive processes, experienced leadership and staff and an effective governance to create a broad support base and backing of its members. The management organisation also needs to build trust and an open working relationship with the Belgian Defence stakeholders.

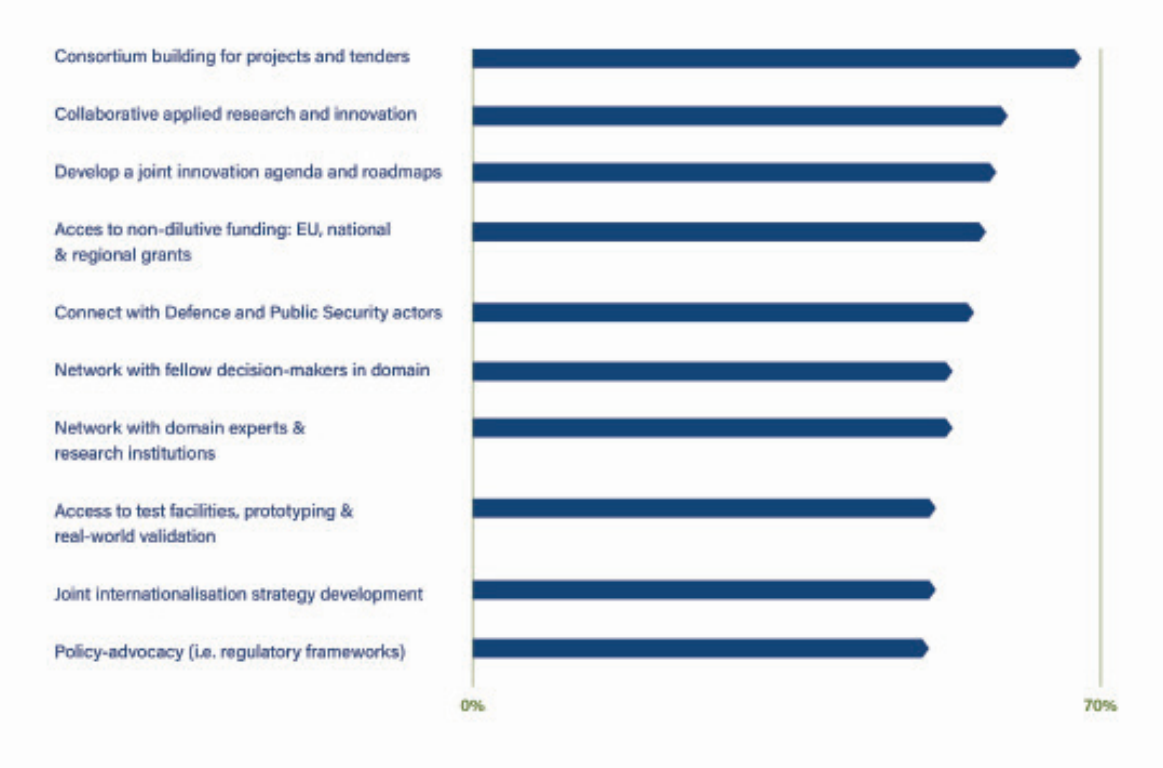
I. TALENT AND TRAINING

Improving access to talent and providing joint training programmes are mentioned as potential operational values of the ecosystem, but appear less prominent than the other categories. Specific training via simulators or crew training is mentioned by individual companies. The need for knowledge about military procedures is also emphasised.



5.4 Priority ranking of RTI ecosystem value drivers by respondents

During the depth interviews, respondents listed the following prioritised top-ten expectations regarding the proposed Research, Technology, and Innovation (RTI) ecosystem:



Priority ranking of RTI ecosystem expectations

This list of priority expectations from the ecosystem aligns very well with the findings of the qualitative depth interviews. As the majority of the respondents are technology and solution providers, many of them SMEs, there is high emphasis on services that accelerate and de-risk joint innovation, that facilitate access to strategic know-how, testing grounds and innovation funding and that lower the barrier of structural engagement with defence, asset owners and operators.

5.5 Buy-in of stakeholders

Throughout the depth interviews, we noticed a strong level of interest in the potential role and establishment of an RTI ecosystem. Whether this general interest and willingness to participate translates in a true engagement, is highly dependent on how the ecosystem is shaped and managed. Important elements listed by several stakeholders are summarised below:

- Concrete projects and demand-driven approach, not a "talking shop";
- Active involvement of government/defence with clear requirements, resource allocation (budget, time, personnel);
- Transparency in the functioning of "the system" (communication, funding procedures, project selection);
- Agility and speed through light and lean procedures with short lead times;
- Neutral ecosystem management organisation;
- Funding for higher TRLs and market valorisation;
- Facilitating collaboration, matchmaking and complementarity between players ("bringing pieces of the puzzle together");
- Support for market access and internationalisation and export of homegrown solutions;
- Access to the defence market ("getting over the wall");
- Test beds;
- Addressing barriers, helping to navigate and resolve obstacles such as security clearances and legal proceedings;
- Value for own organisation/business.

CONCLUSION

Belgium possesses a strong foundation in science, technology, and innovation, supported by world-class universities, strategic research centres, and dedicated innovation hubs, positioning the country at the forefront of maritime innovation. The technology landscape for Critical Maritime Infrastructure Protection (CMIP) is broad and dynamic, covering fixed and mobile surveillance systems, autonomous vehicles (UAVs, USVs, AUVs), robotics, integrated safety and security systems, advanced communications, and AI-driven analytics. Numerous Belgian companies and research organisations are active across these domains, creating fertile ground for ecosystem development.

Strategic initiatives such as DEFRA and collaborative research projects illustrate a strong commitment to transforming research into actionable solutions and commercial opportunities, including the potential creation of start-ups. The insights gathered from the stakeholder landscape confirm a clear and strong consensus on the need for a dedicated Research, Technology, and Innovation (RTI) ecosystem to protect critical maritime infrastructure. Stakeholders from defence, industry, research, and government share a vision of a mission-driven, collaborative, and agile ecosystem that accelerates innovation and bridges the gap between R&D and operational deployment.

The stakeholder analysis further reveals a demand for strengthened collaboration, knowledge sharing, and resource pooling within the ecosystem. Stakeholders expect the CMIP innovation ecosystem to facilitate networking, accelerate technology transfer, and support the commercialisation of research outputs in a transparent, agile and neutral way.

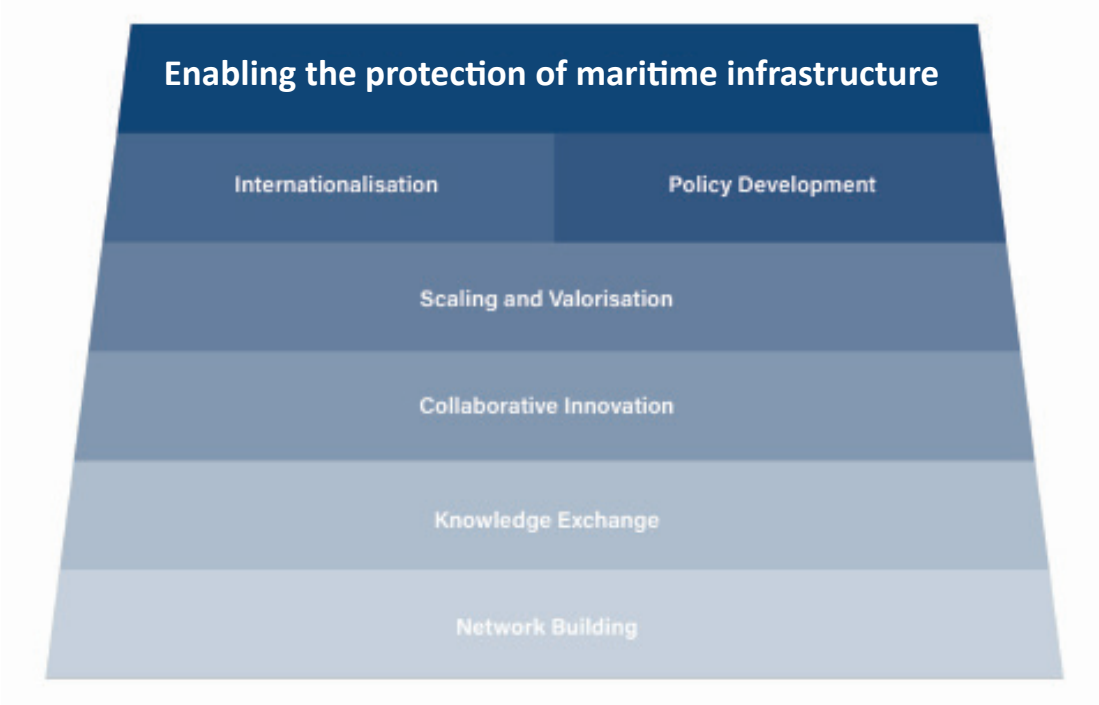
To fully realise the ecosystem's potential, it is critical to maintain an overview of ongoing research, identify opportunities for applied innovation, and foster connections between scientific excellence and industrial application. Building advanced manufacturing capabilities, as exemplified by Flanders Make, will be essential for scaling production and maintaining competitiveness in a rapidly evolving global landscape.

However, unlocking this potential depends on the ecosystem's ability to integrate resources effectively and scale innovation through trust-based partnerships and aligned incentives.

6. Value drivers and services of the ecosystem

6.1 CMIP ES services portfolio

On basis of the concept and experience of the spearhead clusters in Flanders (i.e. Blue Cluster) and the prioritised value drivers and services by the respondents of the depth interviews, the CMIP ecosystem should address the following activity domains:



A. NETWORK BUILDING

Networking is the basis of a collaborative ecosystem, fostering relationships and channels for communication among all stakeholders. The following activities could be deployed to develop a vibrant, dynamic and broad-based network of industry, public sector, research institutions and defence.

Thematic workshops: Organise regular workshops focused on specific threats (e.g. cyber-attacks on port systems, underwater sabotage, environmental hazards), technologies (e.g. AI for anomaly detection, advanced sensor systems), or relevant policy developments. These will build trust and familiarity among diverse actors, facilitate informal information exchange and identify common challenges. These activities provide a low-barrier entry point to engage new participants to the CMIP ES whilst acting as ideation ground for the other activity domains.

Annual CMIP summit: Host a larger-scale annual event bringing together all ecosystem members. This summit should feature keynote speakers from defence, government and industry, panel discussions on strategic challenges, and dedicated breakout sessions for focused networking on emerging threats and solutions. This provides an opportunity to have high-level strategic discussions, showcasing national capabilities, attracting international partners, and setting the annual agenda for collaborative efforts.

Online collaborative portal: Establish and maintain secure digital platform (e.g. an extranet, dedicated forum, or collaborative workspace) where members can share best practices, post research findings, discuss operational challenges, and solicit input from others in real-time. This will facilitate continuous engagement, break down communication barriers and create a searchable repository of knowledge, and enables rapid information dissemination without creating an information overload.

Thematic groups and task forces: Form specialised, project-based thematic groups or task forces addressing specific challenges, e.g. standardisation of subsea cable protection protocols, development of a joint response plan for major port cyber incidents. This helps to drive tangible outcomes, fosters deep collaboration on specific issues, builds specialised expertise, and allows for agile responses to emerging threats.

Cross-sectoral simulation exercises and in-situ demonstrations: Organise multi-agency, multi-company exercises and demonstrations simulating various CMI security incidents (e.g. cyber-attack on a wind farm control system, physical sabotage of a subsea cable, response to an unannounced vessel in a restricted area). This will include joint exercises between the Belgian Navy, port authorities, CMI asset owners or operators, and technology providers to test emergency response protocols. These exercises will help to test interoperability, identify gaps in communication and procedures, assist in future response coordination and enhance mutual understanding of capabilities and limitations. Considering the high resource intensity in creating realistic and challenging scenarios, in the coordination of all participants and stakeholders, in the actual execution, in securing classified information, and in the effective evaluation, these exercises will need extensive and lengthy preparation, advanced project management and extensive stakeholder buy-in and commitments.

B. KNOWLEDGE SHARING

Effective knowledge sharing ensures that lessons learned, best practices, and new insights are disseminated and absorbed effectively across the ecosystem. This could be facilitated in various ways:

Centralised knowledge repository: Develop and maintain a secure, accessible repository of relevant documents, including threat intelligence reports, vulnerability assessments, best practice guidelines, technological white papers, and regulatory frameworks. This could include a digital library containing risk assessments for different types of maritime infrastructure, a database of validated security technologies and reference documentation of international use cases and know-how. Access to such repository could be differentiated in function of information sensitiveness, security clearances, membership categories and participation levels.

Regular threat intelligence briefings: Conduct periodic briefings by defence and security actors (e.g. Maritime Information Crossroads (MIK), National Crisis Centre, Cyber Command) to share the latest maritime threat intelligence, including emerging vulnerabilities, attack vectors, and geopolitical developments. This could include a monthly unclassified briefing on global maritime security trends and their potential impact on Belgian CMI, or a more restricted briefing on specific threats.

Post-incident analysis: Facilitate structured sessions after real-world incidents or significant exercises to analyse what happened, identify root causes, assess response effectiveness, and document lessons learned. This could for example include a debriefing session following a simulated port intrusion to identify areas for improvement in security protocols and communication. This drives a culture of continuous improvement in security practices, prevents recurrence of similar incidents and fosters a culture of learning and accountability.

Expert exchange programmes: Facilitate expert exchanges between different organisations within the ecosystem. For example, a cybersecurity expert from a port authority spending time with a defence cyber unit, or a naval officer shadowing operations at an offshore wind farm control centre. This will deepen the understanding of different operational contexts, builds personal relationships, transfers tacit knowledge, and fosters cross-organisational understanding.

C. INNOVATION

Collaborative innovation programmes are a crucial pillar in the mission of the CMIP ES to develop new solutions, enhance the competitive strengths of the Belgium-based industry and research capabilities and counter evolving threats towards better CMI resilience. The strategic reference for the innovation programme is embedded in the **technology roadmap for R&D and innovation**. This could entail:

Roadmap development: Through collaborative workshops and discussions with experts from within and outside the ecosystem, the ecosystem will act as the central orchestrator of the technology roadmap, ensuring alignment and integration across all stakeholders. It facilitates workshops where diverse perspectives are brought together, conflicts are resolved, and a shared understanding of the roadmap is built. This collaborative process ensures that the roadmap is not just a collection of technologies, but a coherent strategic plan. It helps identify gaps in current capabilities and future needs, guiding focused innovation investments. For more details on the roadmap approach, refer to chapter 7.7.

Joint innovation programmes: On basis of the priorities and phasing defined in the roadmap, collaborative innovation programmes will be launched. These programmes should be focused on specific CMIP challenges, pooling resources and expertise from companies, research institutions, and defence/security agencies. This could for example include research into AI-powered anomaly detection for underwater surveillance, development of resilient communication systems for offshore platforms, specific technologies and approaches for accelerated repair of damaged underwater infrastructure. Through access to diverse expertise and appropriate innovation funding instruments, participants will share risk in innovation and focus on the development of cutting-edge solutions tailored to Belgian needs, whilst exploiting the potential for dual-use technologies. More information on innovation funding instruments and the innovation project ideation and screening cycle are included in respectively chapters 6.4 and 7.7

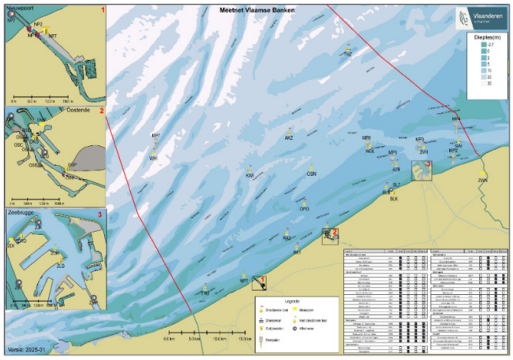
Testbeds and living labs: Facilitate access to dedicated physical or virtual test environments where new CMI protection technologies and methodologies can be rigorously tested and validated in realistic scenarios. These provide a safe space for experimentation, accelerate technology maturation, allows for early identification of practical challenges, and facilitates collaboration between developers and end-users. This could include for example a controlled environment replicating port IT/OT systems for cybersecurity testing, or a designated area in the North Sea for testing advanced underwater drones for surveillance. The provision of a secure cloud environment through the CMIP ES should be considered as an important enabler for collaborative innovation and testing.

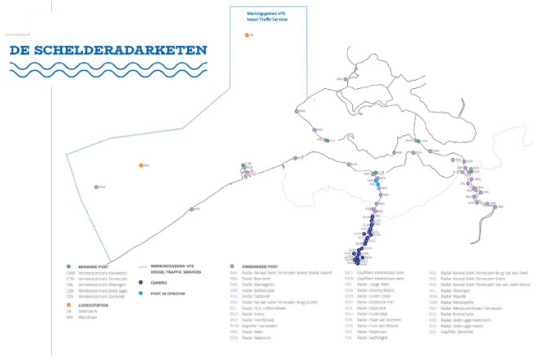
Various future ecosystem partners have expressed interest in the enablement of living labs and test grounds such as Port of Antwerp-Bruges, North Sea Port, Maritime and Coastal Services Agency (MDK) (including ships as floating test ground), Elia, Fluxys and Parkwind. The CMIP ES can facilitate the identification and access to such environment, can support obtaining necessary permits and clearances, ensuring data security within test environments, and attracting sufficient innovative projects.

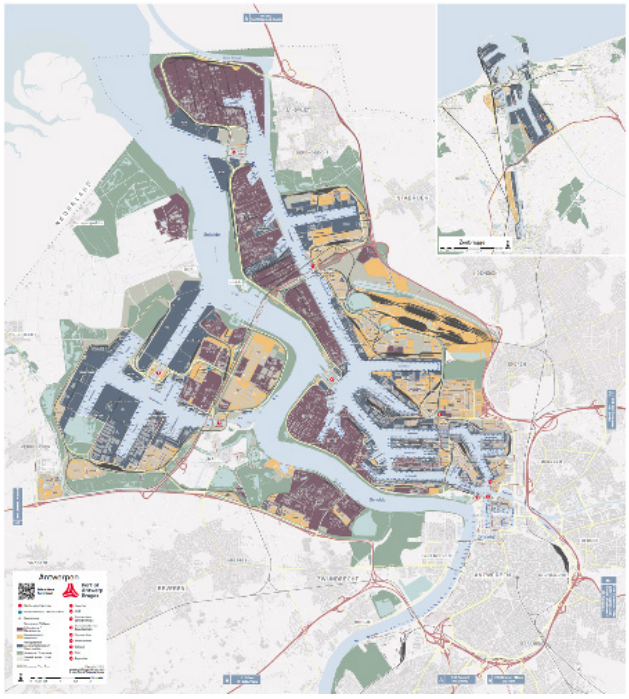
Besides the test ground and living labs environment enabled by the private and public partners mentioned above, the CMIP ES will coordinate with Defence to secure access to (preferably dedicated) military personnel for realistic operational contexts, expert advice and guidance in security clearance and access to exclusive military zones.



MDK infrastructure with potential as a enabling test ground and living labs environment







Port of Antwerp-Bruges with potential as a living labs environment

Technology scouting and horizon scanning: Proactive identification and assessment of emerging technologies globally that could be adapted for CMI protection. This involves monitoring academic research, industry trends, and defence innovations. This could for example include quantum cryptography for secure maritime communications or assessing advancements in satellite imagery for detecting suspicious maritime activity. This will ensure that the ecosystem remains at the forefront of technological capabilities, identifies disruptive technologies early and prevents technological obsolescence.

The roadmap process will include a technology foresight exercise to integrate long-term and disruptive technology trends proactively in the technology roadmap. The scientific domain experts in the steering group and the representatives of the KIs and RTOs will have a particular responsibility to contribute to such broader understanding of the long-term and international horizon.

Innovation challenges: Organise focused events to rapidly prototype solutions to specific CMI protection problems. Larger corporations, i.e. defence system and platform builders, CMI asset owners and operators, will be invited to formulate challenges for SMEs and start-ups. This could for example include tools for faster incident response in port networks, or the design of a cost-effective sensor for small vessel detection in offshore wind farm exclusion zones. This will foster rapid ideation and prototyping, will engage a broader talent pool (including start-ups and individual innovators) in matchmaking and can generate unexpected solutions for future innovation programmes.

Through collaborative workshops and discussions with experts from within and outside the ecosystem, the ecosystem will acts as the central orchestrator of the technology roadmap, ensuring alignment and integration across all stakeholders. It facilitates workshops where diverse perspectives are brought together, conflicts are resolved, and a shared understanding of the roadmap is built. This collaborative process ensures that the roadmap is not just a collection of technologies, but a coherent strategic plan. It helps identify gaps in current capabilities and future needs, guiding focused innovation investments. For more details on the roadmap approach, refer to chapter 7.7.

D. SCALING AND MARKET VALORISATION

Beyond innovation, the ecosystem needs mechanisms to help derisking the scale-up solutions and ensure their commercial viability and wider adoption. The following services are envisaged to contribute to a strong and competitive Belgian industry and business.

Incubator/accelerator programmes for CMIP start-ups: Support the growth of start-ups developing CMI protection technologies through mentorship, funding access, and connections to end-users. The CMIP ES will connect start-ups with relevant and established incubators and accelerators such as imec.istart, IGNITY (key partner and Belgian accelerator site for NATO/DIANA programme, EUDIS Business Accelerator and Matchmaking programme), Incubators.brussels, and Start It @KBC. Over time, the CMIP ES could also establish a dedicated accelerator programme for CMIP start-ups, or an incubator providing lab space and technical guidance for companies developing subsea robotics.

Access to funding and investment networks: Connect innovative companies with relevant national and European funding programmes (e.g. DEFRA, VLAIO, European Defence Fund, Horizon Europe) and private investors. This could include the organisation of pitch events for CMIP start-ups to venture capital firms, or providing guidance on applying for EU defence innovation grants to secure necessary capital for innovation and commercialisation.

Venture building: The CMIP ES will explore options to develop in partnership with Belgian or international corporates, spin-outs or new Belgium-based ventures in highly innovative niche systems for CMIP.

Market intelligence and opportunity mapping: Provide insights for the CMIP ES participants into market needs, regulatory requirements, and procurement processes to help companies tailor their solutions and identify commercial opportunities within Belgium and internationally. This may also include regular monitoring and reporting on relevant calls and tenders and mapping of procurement cycles of public and private CMI asset owners, defence actors and Tier1 system vendors and platforms.

Pre-commercial validation: Bridge the gap between R&D and full-scale deployment by facilitating pre-commercial validation where validated technologies can be implemented in operational CMI environments. This provides real-world validation, gathers essential feedback for refinement, builds confidence among potential end-users, and demonstrates tangible benefits.

Individual growth trajectory support: For selected highly promising start- and scale-ups, a tailor-made support and business coaching programme will be offered with the involvement of experts and staff of the CMIP ES including baselining and regular progress monitoring across various business dimensions.



Pre CMIP ES support baseline assessment
Post CMIP ES active individual growth support

E. INTERNATIONALISATION

International collaboration and scaling is critical given the limited Belgian defence and CMIP markets, the transboundary nature of maritime threats and the need to leverage global expertise and markets. The ES will support its members in different ways.

Participation in international forums and initiatives: Actively engage in relevant international organisations, working groups, and platforms focused on maritime security and critical infrastructure protection. This could include among others participation in NATO maritime security initiatives (i.e. DIANA), EU Coast Guard Forum, or bilateral security dialogues. This allows to influence international standards and policies, share and promote Belgian expertise, gain insights into global best practices and emerging threats, and foster relations with similar ecosystems and clusters in other countries and regions.

Bilateral and multilateral collaboration projects: Initiate and participate in collaborative projects (e.g. EDF and Horizon Europe) with international partners (e.g. specific countries, EU agencies and/or research consortia) on CMI protection. This could include joint research with Dutch RTOs on North Sea subsea cable protection, or collaborative development of maritime surveillance technologies with a Scandinavian partner. This will enhance access to complementary expertise and resources, shared development costs, increased resilience through coordinated security measures, and access to new markets.

Export promotion and market access support: Assist Belgian companies in exporting their CMI protection technologies and services to international markets. (Co-)organise trade missions to countries with significant maritime infrastructure, providing market intelligence on international procurement opportunities, or facilitating introductions to potential international partners in close collaboration with the specialised agencies such as FIT, AWEX and hub.brussels.

Knowledge exchange with international counterparts: Facilitate structured knowledge exchange programmes and visits with foreign defence, security, and infrastructure operators. This could for example include delegation visits of international port authorities to Belgian ports to learn about their security architectures. This allows for benchmarking against international best practices, learning from diverse operational experiences, and identifying areas for mutual improvement.

Joint product development: Build international consortia combining complementary expertise and product know-how. This should result in strategic long-term collaboration and potential joint ventures to bid for international tenders, i.e. in the context of NATO, European and intergovernmental joint defence coordination and procurement organisations such as NATO Support and Procurement Agency (NSPA), NATO Communications and Information Agency (NCIA), Conference of National Armaments Directors (CNAD), European Defence Agency (EDA), European Defence Fund (EDF), Organisation Conjointe de Coopération en Matière d'Armement (OCCAR) and Permanent Structured Cooperation (PESCO).

F. POLICY

The ecosystem can play a vital role in informing and shaping robust policy frameworks for CMI protection at national and international levels in different ways.

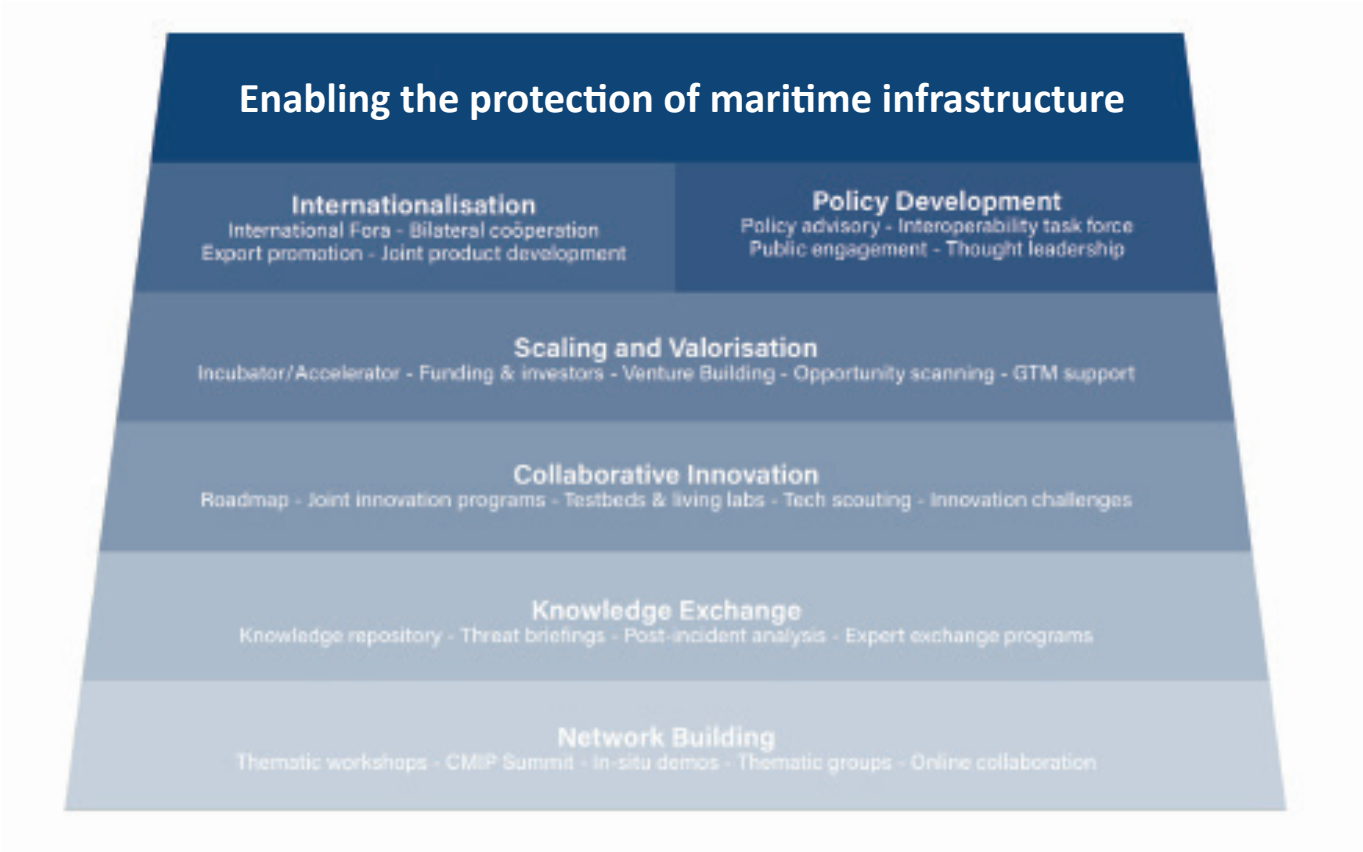
Policy recommendations and advisory services: Provide expert advice and well-researched policy recommendations to government bodies on maritime security and critical infrastructure resilience. This could include for example the development of a white paper on roles and responsibilities in the protection of CMI, or advising on the implementation of EU directives on critical entities resilience (CER Directive) and network and information security (NIS2 Directive).

Regulatory harmonisation and interoperability standardisation advocacy: Advocate for the harmonisation of national and international regulations and the adoption of common security standards to improve interoperability and efficiency. This could reduce the administrative and regulatory burden for operators, enhance cross-border cooperation and strengthen overall regional security, and will facilitate international upscaling.

Campaigns and stakeholder engagement: Raise public and political awareness about the importance of CMI protection and the evolving threats. Support public campaigns explaining the vital role of ports and offshore wind farms, or support parliamentary briefings highlighting the economic and security risks of CMI vulnerabilities. This will help build public support for necessary investments, encourages responsible behaviour and mobilises political will for policy changes.

Input to national security strategies and defence planning: Contribute expert insights to the maritime component of Belgium's national security strategies, defence policy documents, and long-term planning for defence capabilities related to maritime security. This will ensure that national defence and security planning adequately addresses CMI protection needs, aligns resources with strategic priorities, and integrates civilian and military capabilities.

Through the combination of these services, the CMIP ES will realise its mission to enable the protection of maritime infrastructure.



6.2 Specific focus on SMEs, start-ups and scale-ups

Start-ups and innovative SMEs (iSMEs) are the engines behind the fast introduction of new technology. Europe has built one of the best start-up ecosystems in the world. Engaging start-ups for defence, security and resilience capabilities in general and CMIP has the following advantages:

- **Accelerating Innovation and Disruption**: Start-ups and iSMEs are agile and excel in high-risk, high-reward R&D, often outpacing traditional defence contractors and corporates in developing cutting-edge technologies like AI, quantum computing, and autonomous systems. Their speed and willingness to disrupt the status quo can help to rapidly adopt transformative solutions critical for maintaining a technological edge;
- **Cost-Effective**: Start-ups often operate with leaner structures and product-oriented models, enabling them to deliver scalable, commercially priced solutions. This approach can reduce costs while enhancing operational capabilities, making innovation more accessible and budget-friendly;
- **Strengthening the ecosystem**: Collaborating with start-ups diversifies the industrial base, reduces dependency on traditional suppliers, and strengthens supply chain resilience. This not only bolsters national security but also fosters economic growth by supporting local innovation ecosystems. While the classical defence and security players build products that comply with requirements; start-ups and iSMEs test the boundaries of what is possible. We need both;
- **Bridging Technology Gaps**: Start-ups can address gaps in existing capabilities by integrating emerging technologies into legacy systems or introducing entirely new functionalities. For example, U.S. initiatives like DIU have shown how start-ups can rapidly prototype and deploy solutions tailored to short term defence needs;
- **Global Competitiveness and Strategic Alliances**: Engaging with start-ups aligns with global trends in defence and security innovation. These partnerships ensure Belgium remains competitive on the global stage while fostering alliances with like-minded nations.

Investing in start-ups is not just an opportunity for economic growth but also a necessity to future-proof Belgian CMIP against evolving threats and technological challenges.

DO WE HAVE THE RIGHT PLAYERS AND DEAL FLOW?

Start-ups and iSMEs come from different sources: from spinouts from universities and RTOs to creative entrepreneurs that are passionate about finding solutions to our challenges while catching the next business opportunity.

In Belgium we see a very rich ecosystem of university spin-offs as well as entrepreneurs that are supported by a financing & coaching community. Blue Cluster already hosts a number of start-ups and iSMEs in its ecosystems that will contribute to the future of our CMIP capabilities and who will benefit from the growth opportunities. Examples are:

- e-Bo enterprises: secure communication, AI (situational awareness);
- Exosens: underwater vision, sensors and detectors across entire spectrum;
- dotOcean: sensor fusion for situational awareness;
- Exail Robotics Belgium: USVs, sonar detection;
- Marlinks: DAS fingerprinting of vessels and subsea objects in vicinity of subsea cables;
- MAHI: situational awareness, autonomous navigation and remote operations of USVs;
- Senhive: airspace security solutions for drone detection and counter-UAS.

Additionally, **early-stage investors and venture studios** in Belgium are actively scouting for technologies with CMIP potential. The CMIP ecosystem will work with them to identify applications and support commercial deployment.

INTERNATIONAL MOMENTUM AND OPPORTUNITY

Globally, maritime security is seen as a high-growth area. Start-ups like Anduril (USA) and Helsing (EU) are rapidly scaling AI-driven underwater surveillance systems—demonstrating both the potential and urgency of innovation in subsea situational awareness.

Anduril (USA)

Anduril Industries is a U.S.-based private defence technology company founded in 2017 and headquartered in Costa Mesa, California. The company specialises in autonomous systems, artificial intelligence, and robotics, with a focus on serving the U.S. Department of Defence and allied militaries. Its 2024 revenue of $1 billion and over 3,500 employees value the company today at $28 Bio.

In April 2025, Anduril launched Seabed Sentry, an advanced, AI-powered undersea sensor network designed to transform subsea security and surveillance. Seabed Sentry consists of modular, cable-free sensor nodes that can be deployed by autonomous underwater vehicles at depths exceeding 500 meters.

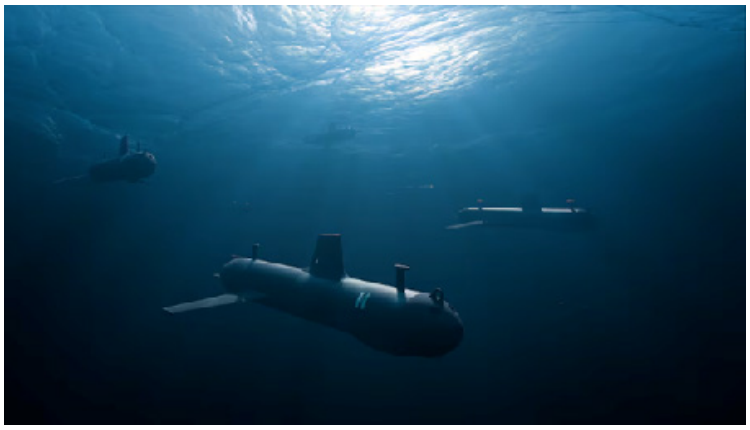


Anduril's Seabed Sentry uses networks of small and low-cost modular sensor nodes.

Helsing (EU)

Helsing is a European defence technology company specialising in artificial intelligence-driven solutions for military and security applications. With a focus on digitalising and securing critical domains, Helsing has rapidly expanded its portfolio from air and land to the maritime sector, leveraging advanced AI and autonomous systems to address emerging threats.

In May 2025, Helsing unveiled its subsea surveillance solution. This integrated system is designed to provide persistent, scalable, and cost-effective underwater monitoring for navies and critical infrastructure protection.



Helsing has launched an underwater drone surveillance network powered by AI

A BELGIAN SUCCESS STORY: GEOXYZ

GEOxyz exemplifies how the Belgian maritime ecosystem nurtures start-ups and innovative SMEs into world class international players. Founded in 1998, GEOxyz began with river mapping projects and evolved into a high-tech data company serving offshore wind projects from Norway to North Africa and the US:

- In just five years, GEOxyz grew from €35 million to €153 million in turnover, with expectations to double again soon;
- The company employs 730 people and is a leader in marine site investigation, asset integrity, and digital innovation, including robotics and drones for data collection and maintenance;
- GEOxyz's success is rooted in a dense network of knowledge institutions, government support, and a culture of continuous improvement and sustainability.



GEOxyz grew from a start-up into an international player with a fleet of 30+ vessels

WHAT START-UPS NEED FROM THE CMIP ECOSYSTEM

To successfully participate in the CMIP market, start-ups need tailored ecosystem support. Key needs include:

- ***Validation*** – Help understanding the operational challenges of CMIP and aligning technology with end-user needs;
- ***Speed*** – Fast feedback loops with operators and quicker pilot-to-deployment cycles;
- ***Guidance*** – Support navigating defence/security regulations, procurement procedures, and compliance requirements;
- ***Transition support*** – Assistance moving from prototype or pilot to full-scale operational adoption;
- ***International access*** – Leverage ecosystem partnerships to unlock access to global markets and flagship projects.

The CMIP ecosystem will actively connect start-ups to:

- Generic start-up services (e.g. finance, coaching, incubation) via imec.istart, Hubs4Growth (including Wintercircus and The Beacon), Start it @KBC, W.IN.G by Digital Wallonia, NEST'Up (Wallona, Co.Station Brussels), BeCentral (Brussels) etc.;
- CMIP-specific partners and clients by **matching technology capabilities to real-world operational needs**.

For many start-ups, CMIP will be a new market or even a new ecosystem they will have to operate in. One of the critical success factors for CMIP start-ups and SMEs is **access to international market**. The CMIP ecosystem will leverage its international relations and partnerships with similar organisations worldwide and its **large corporate members** to provide access to international markets, projects, and partnerships.

ECOSYSTEM AS COLLABORATION ENABLER

Start-ups, iSMEs, and large corporates have complementary strengths, but also different cultures and timelines. The CMIP ecosystem will actively facilitate trust-based partnerships and de-risked collaboration models by:

- Clarifying shared objectives (technology fit, go-to-market strategies, etc.);
- Creating neutral ground for co-development and piloting;
- Supporting financing and validation mechanisms;
- Avoiding pitfalls like exclusivity traps, funding delays, or subcontractor treatment.

Start-ups gain access to markets, clients, and credibility. Corporates gain access to agility, talent, and breakthrough innovation. The CMIP ecosystem will bridge the gap between the two and provide a structured framework for collaboration.

Flanders and Belgium are already fertile ground for maritime innovation. With a strong base of start-ups, research excellence, corporate partners, and forward-looking investors, the CMIP ecosystem can serve as a launchpad for the next generation of global maritime security leaders.

6.3 Ecosystem of ecosystems

Given the specific nature and the different and diverse areas of expertise of the European and international players in CMIP, it is key to connect and join forces with other ecosystems that are active on maritime security. Not only can we learn from those ecosystems, but we will also provide mutual access to our partners and off-takers to create an aggregated market with sufficient scale. In addition, the connections and collaborations with other EU ecosystems help to build trust and the working relations that are ideal to bring our ecosystem partners together in international projects such as the ones organised by EDF.

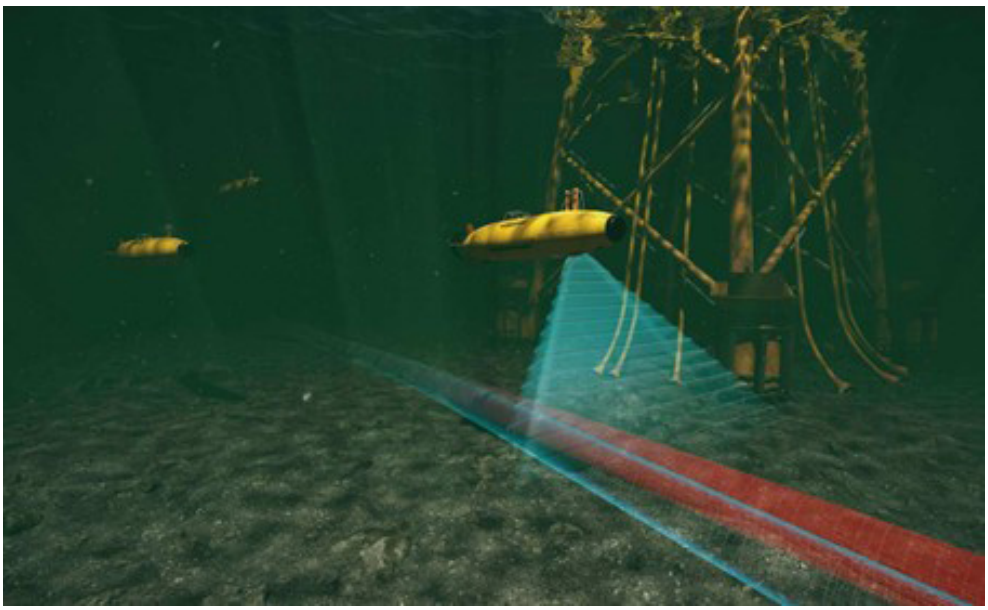
Based on a first screening of clusters and projects, publications and media presence (like the Marsec conference), we have identified a non-exhaustive list of ecosystems that will strengthen our work and impact:

Sweden: Marine Technology Center of Sweden

The Marine Technology Center of Sweden works for a safe and green Europe. With a focus on marine energy, defence and sustainable marine environments. It is an ecosystem that inspires innovation and growth in marine technology.

Germany: Ocean Technology Campus Rostock

With an active department of Fraunhofer IGD in Rostock and top partners such as Partner North.io, a specialist in maritime geodata, the Ocean Technology Campus aims to strengthen the German marine technology by opening up important markets and providing impulses for a worldwide knowledge-based sustainable use of the oceans. Rostock is one of Germany's most traditional maritime locations with an exceptionally high density of marine and maritime research.



North.io links satellite and ship position data and visualises the position of CMI

Finland: Hybrid CoE

Hybrid CoE is an autonomous, network-based international organisation countering hybrid threats. CMIP is one of the key areas they cover. The Centre is unique in the sense that it is the only actor having both the EU and NATO work and conduct exercises together, with activities covering a wide range of domains from civil to military, and from hostile influencing to hybrid warfare. Their research and recommendations are valuable for all ecosystem partners.

France: Pôle Mer Mediterranéé

The Mediterranean Sea Cluster offers services that support the innovation and growth of maritime stakeholders. The cluster has strategic actions in the field of Defence, Security and Maritime Safety around 4 challenges:

- The exploitation of maritime data: informational superiority and optimal exploitation of data;
- Optimising the human factor through automation to better explore and protect the ocean;
- Improving maritime surveillance and security;
- Improving resilience at sea and environmental safety.

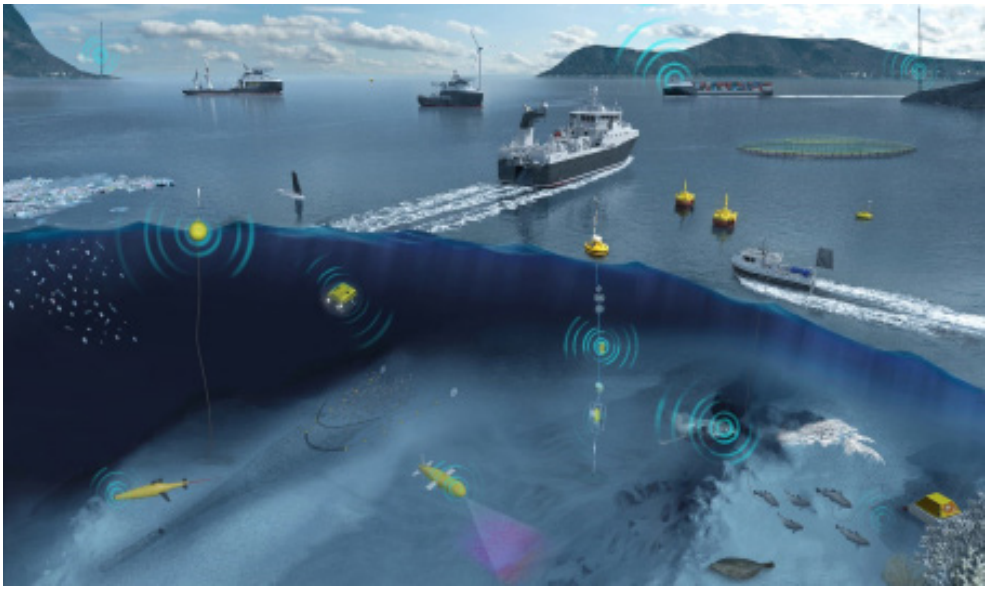
Members who are also active in Belgium include Exail, Naval Group and Thales.

Norway: Kongsberg Innovasjon

Kongsberg Innovation is an incubator owned by industry that launches new companies, many of them in the maritime sector. They have developed the processes, network and know-how and work with start-up companies from Norway and abroad.

Norway: Fjordlab

Fjordlab is a collaboration between the Norwegian University of Science and Technology's Applied Underwater Robotics Laboratory (AUR lab) and OceanLab.



Fjordlab Alesund activity overview

The Netherlands: Campus@SEA and SEASEC

The Seabed Security Experimentation Centre (SeaSEC) is located in The Hague close to Campus@Sea in the port of Scheveningen. Campus@Sea does research and innovation about the protection of subsea infrastructure such as data and energy cables.

Denmark: BlueTech center

The Danish BlueTech Center is engaged in an Interreg project with Germany and has a clear focus on maritime AI. Given the importance of digital twins, data and AI for maritime situational awareness in CMIP, it will be key to connect to this ecosystem and the partners involved in the project. The following chart gives an overview of the different partners that join an ecosystem or project with a focus on maritime AI.



Project Partners and Competence Areas Maritime at the Danish BlueTech Center

ChainPORT

ChainPORT is a cross-national partnership among the world's leading ports (Singapore, Busan, Hamburg, Rotterdam, Port of Antwerp-Bruges, Barcelona, Goteborg, Montreal, Los Angeles, ...) which enables maritime stakeholders through innovation and digitalization to achieve secure, efficient, and sustainable door-to-door supply chains. Driven by innovation and collaboration, these major maritime players work on best-in-class cyber resilience standards, safe access to ports, sustainable shipping, etc.

Connectivity

The list of ecosystems in the domain of maritime security is certainly not limited to the above selection and once the Belgian CMIP ecosystem becomes operational, it will be key to identify the peer ecosystems to join forces with to have a bigger and faster impact. Still, even the limited list which we just described, shows the interest and momentum in this space and gives us the confidence and comfort that there is already a solid basis for joining and contributing to these European efforts with the best of breed partners from our Belgian CMIP ecosystem. One of the key roles of the Belgian CMIP ecosystem will be to create, manage and leverage the relations with the peer ecosystems in Europe and worldwide.

At the NATO level, the **DIANA initiative** is an important lever to lift Belgian innovation solutions for defence (dual-use) to a European-Transatlantic level. Besides the limited funding provided for in DIANA calls, access to international defence partners and guidance from the DIANA team are important elements. The Ecosystem Management Organisation (EMO)'s role is to support and guide SMEs in building and submitting quality and relevant cases to this platform.

6.4 Access to innovation financing instruments

A key component of the CMIP ecosystem is support and facilitation in the area of financing. The ecosystem plays an active role in identifying, unlocking, and guiding access to existing funding instruments relevant to the fields of defence, security, and dual-use technologies.

The ecosystem will provide targeted support in accessing well-known European, international, and national funding mechanisms, such as EDF, EDA, NATO Diana, DEFRA and other relevant programmes such as Horizon Europe or even Interreg programmes.

The CMIP ecosystem can support companies, research institutions, and public stakeholders in navigating this funding landscape, and in forming the right partnerships and consortia to participate successfully in these programmes.

INNOVATIVE FINANCING MECHANISMS

In addition to existing channels, the ecosystem also sees a role in exploring, co-developing, and testing new financing instruments in collaboration with the relevant authorities. These instruments can address specific needs within the dual-use innovation field, where traditional financing models may fall short.

The models described below serve as inspiration for the types of instruments that could be integrated into the ecosystem. They are not detailed versions of existing programmes but offer a foundation for future policy development and indicate where the ecosystem members are looking for:.

Must Have

1. Innovative Procurement
This model focuses on demand-driven innovation, based on the concrete needs and challenges of end users. The goal is to enable a flexible and accelerated transition from procurement to prototype development—typically through short cycles of 6 to 9 months, centred on rapid prototyping and iteration. Unlike grants, this approach constitutes a direct purchase, which significantly increases its value for start-ups, particularly in terms of financing and revenue potential. Moreover, the regulatory framework for this model already exists at the EU, Belgian and Flemish levels.

2. Rapid Technology Prototyping
This model focuses on fast and cost-efficient testing of promising new technologies through short-term projects with a fixed budget per partner. It enables quick validation of emerging technologies and is well suited for the rapid development of innovative solutions in a defence context, without long-term commitments.

3. Staged Contracts
These contracts are a phased funding model in which projects are evaluated in successive stages, such as concept papers, full proposals, and pilot projects. The structured approach allows for the early identification of promising innovations while minimising risk. It facilitates the controlled integration of new technologies into broader government programmes and supports targeted investments in high-impact solutions. A specific application of this model is Milestone-Based Competitions, where projects are divided into clearly defined, technically feasible milestones, with funding released only upon successful completion of each stage. This incentivises innovation, particularly among small businesses and start-ups, while safeguarding public funds by tying investment to concrete results

4. Projects Close to Market Introduction (TRL8)
The aim is to develop funding models focused on projects nearing market introduction. This type of instrument would be ideal for systems or products that are already technically proven in a realistic environment. The risks for investors or governments are significantly lower, as the technology is ready for deployment. This opens up possibilities for faster and more efficient integration, for example in a defence context, avoiding long development trajectories.

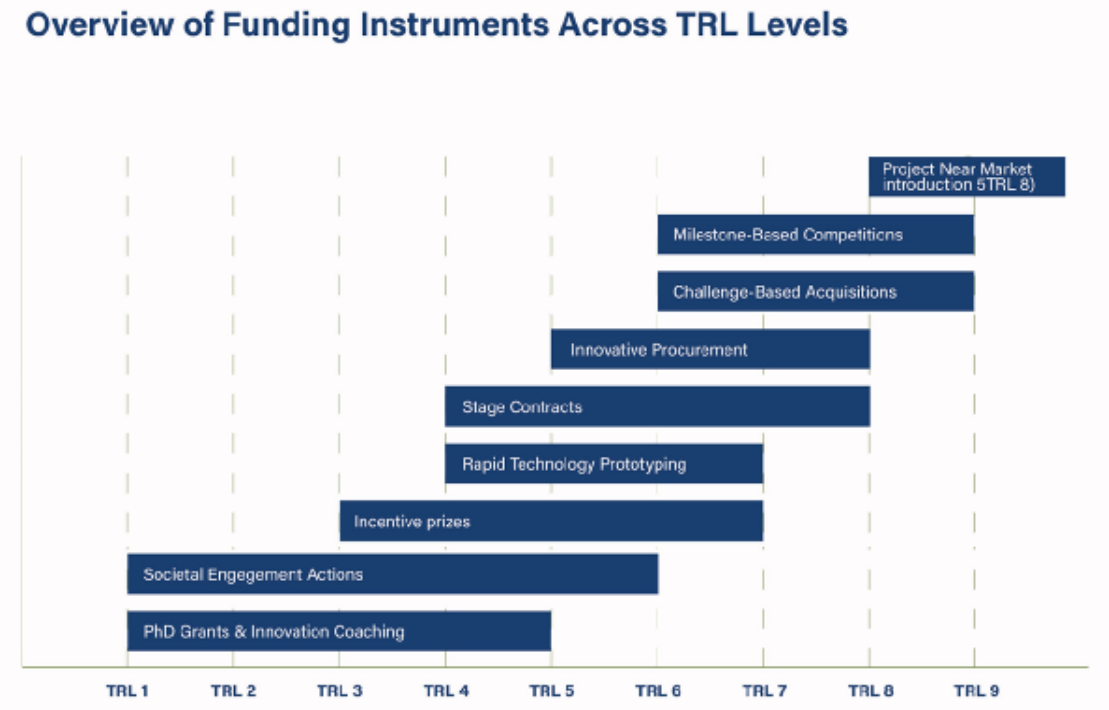
Nice to Have

5. Challenge-Based Acquisitions
Private sector companies are challenged to demonstrate their solutions in real-world conditions. This model encourages a "try before you buy" approach and allows for fast and cost-effective integration of innovative technologies into existing programmes. For example, this could facilitate the adoption of defence innovations through real-world challenges, where only successful participants progress to the contract award phase.

6. Incentive Prizes
The use of competitions with both financial and symbolic rewards can stimulate innovation and attract new players. This model encourages open competition to solve specific challenges. It is a powerful tool for sparking innovation, for example by awarding prizes for technological breakthroughs in defence and dual-use applications.

7. Societal Engagement Actions
In addition to the above funding instruments, efforts can be made to foster societal engagement. This could include gamified learning tracks or e-sports competitions that connect students and young talents with dual-use innovation. Platforms for collaboration and awareness can help identify new ideas and attract future talent to the defence and innovation industries.

8. PhD Grants and Innovation Mentorship
For PhD grants in the defence or dual-use domain, a funding model can be developed that includes support during and after the doctoral research. This increases returns on public investment and ensures that the developed knowledge is actually applied. Programmes such as MIT's Innovation X can serve as inspiration, fostering collaboration between universities and defence actors and bringing technological innovations into practical use.



Each bar indicates the TRL range the instrument is suited for:

- **Early Stage (TRL 1–4)**: Focused on fundamental research, early engagement, and academic involvement (e.g. PhD grants, societal engagement);
- **Mid Stage (TRL 4–7)**: Support for applied R&D, prototyping, and milestone-driven innovations;
- **Late Stage (TRL 7–9)**: Emphasis on market readiness, acquisition, and implementation in real-world.

This chapter presents a comprehensive overview of possible activities that the ecosystem management organisation can undertake. *These actions are intended to be implemented progressively, allowing the organisation to adapt to priorities and available resources over time.*

A concrete action plan, outlined in Chapter 10, prioritises and elaborates on many of these proposals. The activities introduced in this chapter will be gradually developed in alignment with strategic needs and organisational capacity.

CONCLUSION

The CMIP ecosystem focuses on six core areas to strengthen maritime infrastructure protection: building a strong cross-sector network; enabling structured knowledge exchange; fostering joint innovation, supporting the scaling and commercialisation of solutions; promoting international collaboration and export; and shaping effective policy frameworks.

Start-ups and innovative SMEs (iSMEs) are essential drivers of rapid, cost-effective innovation in CMIP, bringing agility, disruptive technologies, and economic diversification. Belgium's strong start-up ecosystem—supported by investors, incubators, and organisations like Blue Cluster—already includes promising companies contributing to CMIP. Successful integration into the CMIP market requires tailored support such as validation, speed, regulatory guidance, and international access. The CMIP ecosystem will actively connect start-ups to partners, clients, and global markets, while also fostering trust-based collaboration between start-ups and corporates to accelerate innovation and resilience.

Access to appropriate financing is a crucial pillar of the CMIP ecosystem. The ecosystem will help stakeholders navigate and leverage national, European, and international funding programmes relevant to defence, security, and dual-use technologies. Beyond existing mechanisms, the ecosystem also aims to explore and co-develop innovative financing tools tailored to the specific needs of dual-use innovation, where traditional funding often falls short. The goal is to make funding more accessible and better aligned with the pace and needs of technological development.

7. Recommendations & conclusions

INTRODUCTION

The recommendations below capture the essential actions needed to move from feasibility to implementation. They serve as a concrete foundation for operationalising the proposed CMIP innovation ecosystem and guiding strategic decision-making going forward.

RECOMMENDATIONS

1. Launch a mission-driven "Made in Belgium" innovation ecosystem to accelerate the valorisation of the dual-use market and international upscaling;
2. Create an open collaboration with defence and develop an aligned innovation roadmap;
3. Unite scientific and research communities with start-ups, innovative SMEs, and corporates to strengthen knowledge and provide access to top expertise and talent;
4. Provide access to transparent, lightweight and fast-track innovation funding and access to financing;
5. Develop a lead role in a European "ecosystem of ecosystems" and consortium development for EU and international funding;
6. Prioritise the integration of start-ups and SMEs in (defence) system solutions; leverage champions to become global leaders in the CMIP market;
7. Develop tailor-made value-added services for SMEs and start-ups;
8. Create a living lab and provide access to test infrastructure to speed up innovation processes;
9. Leverage on securing port critical infrastructure with ports as a unique innovation platform for internationalisation;
10. Ensure an EMO governance structure which is independent, agile, and transparent and links to regional and local initiatives;
11. Set up a task force on interoperability
12. Promote economic and societal value of CMI protection with civil society and policy-makers.

In addition to these recommendations, this study suggests to develop high impact projects on:

- Real-time maritime situational awareness (digital twin) of the Belgian North Sea;
- Belgium's niche expertise in drones (UAV, USV, AUV) and valorise its export potential;
- The development of repair capacity to create a first-mover advantage.

8. Annexes

OVERVIEW OF ANNEXES

- Annex 1: List of abbreviations and acronyms
- Annex 2: Strategic actions on the CMIP recommendations
- Annex 3: Market size and growth projections for CMIP

ANNEX 1
List of abbreviations and acronyms

By alphabetical order

AI	Artificial Intelligence
AIS	Automatic Identification System
APAC	Asia Pacific
AUR lab	Applied Underwater Robotics Laboratory
AUV	Autonomous Underwater Vehicle
AWEC	Agence wallonne à l'Exportation et aux Investissements Etrangers - *Wallonia Export & Investment Agency*
BC	Blue Cluster
CAGR	Compound Annual Growth Rate
CER	Critical Entities Resilience
CMI	Critical Maritime Infrastructure
CMIP	Critical Maritime Infrastructure Protection
CMIP ES	Critical Maritime Infrastructure Protection Ecosystem
CNAD	Conference of National Armaments Directors
CNN	Convolutional Neural Network
CoE	Centre of Excellence
DAS	Distributed Acoustic Sensing
DDS	Diver Detection Sonar
DEFRA	Defence Related Research Action
DIANA	Defence Innovation Accelerator for the North Atlantic
DIU	Defense Innovation Unit
DIRS	Defence, Industry and Research Strategy
DNN	Deep Neutral Network
DVL	Doppler Velocity Log
ECDIS	Electronic Chart Display and Information System
ECOOM	Expertisecentrum Onderzoek en Ontwikkelingsmonitoring - *Expertise Centre for Research and Development Monitoring*
EDA	European Defence Agency
EDF	European Defence Fund
EMO	Ecosystem Management Organisation
EU	European Union
EUDIS	EU Defence Innovation Scheme
FIT	Flanders Investment & Trade
FPIM	Federale Participatie- en Investeringsmaatschappij - *Federal Holding and Investment Company*
FTE	Full-Time Equivalent
GDP	Gross Domestic Product
GMDSS	Global Maritime Distress and Safety System
GNSS	Global Navigation Satellite System
GPS	Global Positioning System
Howest	Hogeschool West-Vlaanderen - *University of Applied Sciences West Flanders*
HVAC	Heating, Ventilation and Air Conditioning
IDS	Intruder Detection Sonar
IMEC	Interuniversitair Micro-Electronica Centrum - *Interuniversity Microelectronics Centre*
INS	Inertial Navigation System
IoT	Internet of Things
IR	Infrared
iSME	Innovative Small and Medium-sized Enterprise
ISR	Intelligence, Surveillance and Reconnasisance
IT	Information Technology
KI	Knowledge Institution
KPI	Key Performance Indicator
KU Leuven	Katholieke Universiteit Leuven - *Catholic University of Leuven*
LiDAR	Light Detection and Ranging
LOFAR	Low Frequency Array
MAD	Magnetic Anomaly Detection

MDK	Agentschap Maritieme Dienstverlening en Kust - *Agency for Maritime and Coastal Services*
MIK	Maritiem Informatie Kruispunt – ***Maritime Information Crossroads***
MIT	Massachusetts Institute of Technology
ML	Machine Learning
MoD	Ministry of Defence
MOG	Modular Offshore Grid
MOU	Memorandum Of Understanding
NATo	North Atlantic Treaty Organisation
NCIA	NATO Communications and Information Agency
NIS	Network & Information Security
NLP	Natural Language Processing
NSPA	NATO Support and Procurement Agency
OCCAR	Organisation Conjointe de Coopération en Matière d'Armement - *Organisation for Joint Armament Cooperation*
OT	(1) Operational Technology; (2) Other Transaction
PESCO	Permanent Structured Cooperation
PMV	Participatiemaatschappij Vlaanderen
PoAB	Port of Antwerp-Bruges
PTZ	Pan Tilt Zoom
R&D	Research & Development
R&T	Research & Technology
RADAR	Radio Detection And Ranging
RD&I	Research, Development and Innovation
RF	Radio Frequency
RHID	Royal Higher Institute for Defence
RNN	Recurrent Neural Network
RTDI	Research, Technology Development and Innovation
RTI	Research, Technology and Innovation
RTO	Research and Technology Organisation
Satcom	Satellite Communications
SCADA	Supervisory Control and Data Acquisition
SeaSEC	Seabed Security Experimentation Centre
SG	Steering Group
SLAM	Simultaneous Localisation And Mapping
SME	Small and Medium-sized Enterprise
TRL	Technology Readiness Level
UAS	Unmanned Aircraft System
UAV	Unmanned Aerial Vessel
UGent	Universiteit Gent - *Ghent University*
USV	Unmanned Surface Vessel
VKI	Von Karman Institute for Fluid Dynamics
VLAIO	Agentschap Innovatie & Ondernemen - *Flanders Innovation & Entrepreneurship*
VLIZ	Vlaams Instituut voor de Zee - *Flanders Marine Institute*
VTOL	Vertical Take-Off and Landing
VRT	Vlaamse Radio- en Televisieopmroep - *Flemish Public Broadcasting Company*

ANNEX 2
Strategic actions on the CMIP recommendations

1. LAUNCH A MISSION-DRIVEN "MADE IN BELGIUM" INNOVATION ECOSYSTEM TO ACCELERATE THE VALORISATION OF THE DUAL-USE MARKET AND INTERNATIONAL UPSCALING

RATIONALE:

Belgium's maritime sector possesses a strong base of research, technology, and industrial actors.
These actors play an important role in the setting up of this ecosystem. A mission-driven innovation ecosystem, clearly branded as "Made in Belgium," will harness these strengths to accelerate the commercialisation of dual-use technologies and scale Belgian solutions internationally, taking advantage of the rapidly growing global market for critical maritime infrastructure protection.

KEY ACTIONS:

- Establish a national branding and communication strategy for the ecosystem;
- Identify and launch flagship dual-use innovation projects with export potentia;.
- Set up a central coordination office to support internationalisation and market entry and where possible work together with other actors, such as FIT;
- Facilitate matchmaking events and export consortia for Belgian companies;
- Monitor and report on ecosystem-driven market growth and international deals.

2. CREATE AN OPEN COLLABORATION WITH DEFENCE AND DEVELOP AN ALIGNED INNOVATION ROADMAP

RATIONALE:

Defence is both a key end-user and a source of operational expertise for critical maritime infrastructure protection. Open collaboration ensures that innovation efforts are aligned with real-world security needs and that defence actively contributes to and benefits from the ecosystem's research and innovation agenda.

KEY ACTIONS:

- Formalise defence participation in ecosystem governance and project steering;
- Organise regular co-creation workshops with defence, industry, and research partners;
- Jointly develop and update an innovation roadmap that aligns ecosystem priorities with defence and asset owner needs;
- Pilot and evaluate dual-use technologies in collaboration with defence stakeholders;
- Facilitate secure data and knowledge exchange between defence and civilian partners.

3. UNITE SCIENTIFIC AND RESEARCH COMMUNITIES WITH START-UPS, INNOVATIVE SMES, AND CORPORATES TO STRENGTHEN KNOWLEDGE AND PROVIDE ACCESS TO TOP EXPERTISE AND TALENT

Rationale:

Bridging the gap between research, start-ups, SMEs, and corporates is essential for rapid knowledge transfer, talent development, and the creation of high-impact solutions. A unified community will foster cross-disciplinary innovation and ensure that the best expertise is accessible to all ecosystem participants.

Key Actions:

- Launch joint research and innovation projects with mixed consortia;
- Organise regular knowledge-sharing events, project generation workshops and seminars, and hackathons;
- Establish a platform for networking and resource sharing.

4. PROVIDE ACCESS TO TRANSPARENT, LIGHTWEIGHT AND FAST-TRACK INNOVATION FUNDING AND ACCESS TO FINANCING

Rationale:

Timely and accessible funding is critical to accelerate innovation, especially for SMEs and start-ups. Transparent and streamlined funding mechanisms will lower barriers to entry, speed up project initiation, and attract a broader pool of innovators to the ecosystem.

Key Actions:

- Facilitate access to dedicated innovation funds, including PMV, FPIM;
- Implement rolling calls and fast-track review for urgent or high-potential projects;
- Offer clear guidelines and feedback for funding applications;
- Build a network and facilitate connections to venture capital, public grants, and EU/international funding;
- Publicly track and communicate funding outcomes and success stories.

5. DEVELOP A LEAD ROLE IN A EUROPEAN "ECOSYSTEM OF ECOSYSTEMS" AND CONSORTIUM DEVELOPMENT FOR EU AND INTERNATIONAL FUNDING

Rationale:

Taking a leadership role in European and global consortia will enhance Belgium's influence, unlock access to large-scale funding, and foster cross-border innovation. Building alliances with other ecosystems multiplies resources and impact.

Key Actions:

- Map and engage with leading European and international maritime innovation clusters;
- Proactively initiate and coordinate EU project consortia (e.g. Horizon Europe and EDF);
- Represent the Belgian ecosystem in European cluster/network platforms;
- Share best practices and develop joint demonstration projects with international partners;
- rack and leverage international funding opportunities for Belgian stakeholders.

6. PRIORITISE THE INTEGRATION OF START-UPS AND SMES IN (DEFENCE) SYSTEM SOLUTIONS; LEVERAGE CHAMPIONS TO BECOME GLOBAL LEADERS IN THE CMIP MARKET

Rationale:

Start-ups and SMEs bring agility and innovation but need support for market entry. Integrating them into system-level solutions and connecting them with national champions will accelerate technology adoption and build global leadership.

Key Actions:

- Create dedicated calls for start-up and SME participation in system integration projects;
- Identify and support Belgian "champions" to lead international consortia;
- Provide mentoring, business development, and internationalisation support for SMEs;
- Celebrate and promote success stories to inspire further participation.

7. DEVELOP TAILOR-MADE VALUE-ADDED SERVICES FOR SMES AND START-UPS

Rationale:

SMEs and start-ups face unique challenges in scaling and accessing markets. Tailored services will enhance their ability to innovate, grow, and contribute to the ecosystem's impact.

Key Actions:

- Offer advisory services on certification, compliance, and dual-use regulations;
- Provide shared access to R&D infrastructure and technical expertise;
- Organise targeted training, workshops, and networking events;
- Facilitate access to public and private innovation funding for early-stage ventures;
- Set up an individual growth trajectory and monitoring progress across various business dimensions, such as market intelligence, technology, regulation, team, customers and offtakers, societal and environmental acceptance, industrialisation, supply chain, governance and strategy.

8. CREATE A LIVING LAB AND PROVIDE ACCESS TO TEST INFRASTRUCTURE TO SPEED UP INNOVATION PROCESSES

Rationale: A living lab approach enables rapid prototyping, real-world testing, and iterative improvement of new technologies, reducing development risks and accelerating time-to-market.

Key Actions:

- Establish a network of living lab sites across key maritime infrastructure types;
- Provide open access to testbeds, simulation environments, and operational data;
- Facilitate collaborative pilot and demonstration projects in real-world settings;
- Partner with regulatory bodies to streamline testing and certification;
- Capture and share lessons learned to inform future projects.

9. LEVERAGE ON SECURING PORT CRITICAL INFRASTRUCTURE WITH PORTS AS A UNIQUE INNOVATION PLATFORM FOR INTERNATIONALISATION

Rationale:

Belgium's ports are strategic assets and ideal testbeds for showcasing and scaling CMIP innovations. Using ports as platforms for international collaboration will attract global partners and position Belgium as a reference market.

Key Actions:

- Designate Belgian main ports as international innovation hubs;
- Organise international demonstration events and technology showcases at port sites;
- Facilitate pilot projects with global partners and end-users in port environments;
- Promote successful port-based innovation cases internationally;
- Integrate port authorities into ecosystem governance and planning.

10. ENSURE AN EMO GOVERNANCE STRUCTURE WHICH IS INDEPENDENT, AGILE, AND TRANSPARENT AND LINKS TO REGIONAL AND LOCAL INITIATIVES

Rationale:

A robust, independent, and agile governance model is essential for credibility and effectiveness. Linking to regional and local initiatives ensures broad participation and alignment with identified needs.

Key Actions:

- Establish a multi-stakeholder board with balanced representation;
- Define clear rules for participation, decision-making, and conflict resolution;
- Implement transparent reporting and accountability mechanisms;
- Regularly review and adapt governance processes for agility;
- Foster connections with regional and local CMIP initiatives.

11. SET UP A TASK FORCE ON INTEROPERABILITY

Rationale:

Interoperability is essential for integrating diverse technologies and ensuring seamless operation across national and international maritime systems. A dedicated task force will drive standardisation and compatibility.

Key Actions:

- Convene stakeholders to define interoperability requirements;
- Promote common technical standards and protocols;
- Coordinate with EU and international standardisation bodies;
- Pilot and validate interoperable solutions in joint exercises;
- Promote interoperability as a criterion for project funding.

12. PROMOTE ECONOMIC AND SOCIETAL VALUE OF CMI PROTECTION WITH CIVIL SOCIETY AND POLICY-MAKERS

Rationale:

Broad societal and political support is crucial for sustaining the CMIP ecosystem. Communicating the economic and societal benefits of CMI protection will build trust, attract investment, and inform policy.

Key Actions:

- Launch public awareness campaigns on the importance of CMI protection;
- Engage civil society organisations and local communities in ecosystem activities;
- Organise policy briefings and stakeholder dialogues with decision-makers;
- Publish impact reports demonstrating economic and societal benefits;
- Collaborate with educational institutions to integrate maritime security topics into curricula.

In addition to these recommendations, this study suggests to develop high impact projects on:

- Real-time maritime situational awareness (digital twin) of the Belgian North Sea;
- Belgium's niche expertise in drones (UAV, USV, AUV) and valorise its export potential;
- The development of repair capacity to create a first-mover advantage.

ANNEX 3
Market size and growth projections for CMIP

To estimate the market potential of CMI protection, a two-step approach was applied:

- Top-down analysis: Starting from the total defence budgets of national governments, an estimated share was allocated to maritime security technologies to derive a high-level market estimate.
- Bottom-up analysis: This approach calculated the potential security value based on the presence of critical maritime infrastructure and the estimated deployment of technologies required to secure it (e.g. surveillance systems, cybersecurity, autonomous monitoring, and physical protection solutions).

By combining both perspectives, the analysis provides a robust and balanced view of the potential market size, capturing both strategic-level funding trends and concrete infrastructure-driven security needs.

GLOBAL AND REGIONAL MARKET ESTIMATES

The global market for maritime security technologies is projected to grow from €42 billion in 2025 to €116 billion by 2050, according to the ORTELIUS study. Europe, with its dense offshore infrastructure and advanced regulatory environment, represents a significant share of this market. Investment needs are substantial, with estimates of $1.5 trillion in sovereign and $1 trillion in private funding required globally by 2030 to secure blue economy growth.

SEGMENT ANALYSIS

Surveillance and Detection: Includes fixed and mobile sensor networks, autonomous drones (air, surface, subsea), and advanced radar/sonar systems. These segments are growing at CAGRs of 8–13%, driven by both commercial and defence demand.

Communication and Data Exchange: Secure, resilient networks (including satellite and 5G/6G) are essential for real-time data transfer and remote operations.

Response and Repair: Rapid intervention technologies, such as autonomous repair drones and remotely operated vehicles (ROVs), are emerging as critical tools for minimising downtime and damage.

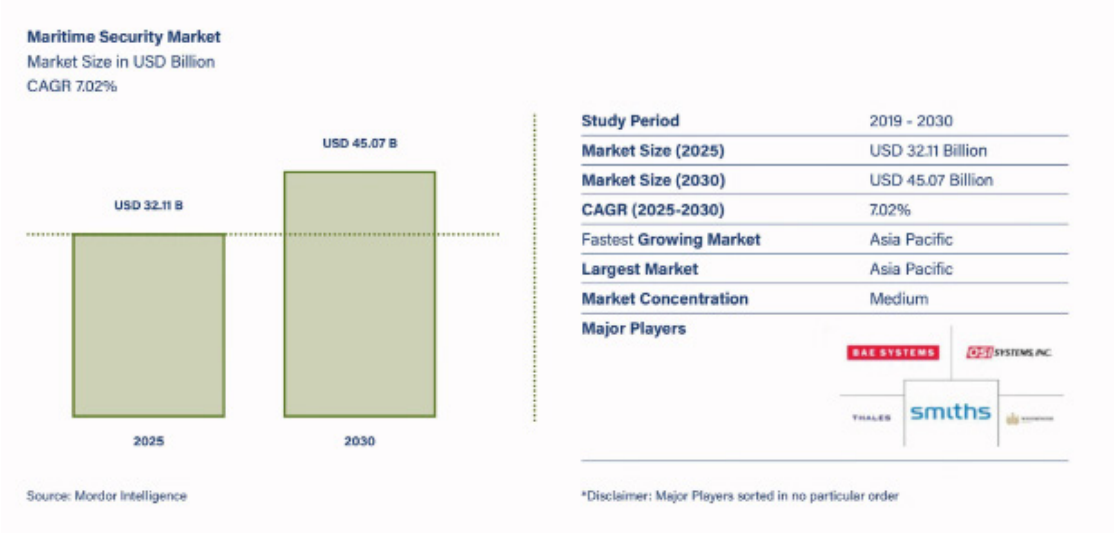
Data Analytics & AI: The maritime AI market is expected to grow at a CAGR of over 40%, reflecting the central role of AI in anomaly detection, threat assessment, and operational optimisation.

TECHNOLOGY ADOPTION AND INNOVATION TRENDS

The integration of digital twins, predictive analytics, and autonomous systems is transforming CMIP. Dual-use technologies—originally developed for defence or offshore energy—are increasingly applied across civil and commercial contexts. The Netherlands and Belgium are recognised for their leadership in repair drones and digital twins, offering a competitive edge in these high-growth domains.

MARKET RECOMMENDATIONS

- Global government spending on maritime defence will at least double in the coming 25 years, with the US remaining a dominant market.
- Global markets for maritime security, including private spending, are expected to grow at a rate of CAGR 7% or more during the next 5 years according to some analyst studies.



Global growth of the maritime security markets according to Mordo Intelligence

PUBLIC SPENDING ON MARITIME DEFENCE

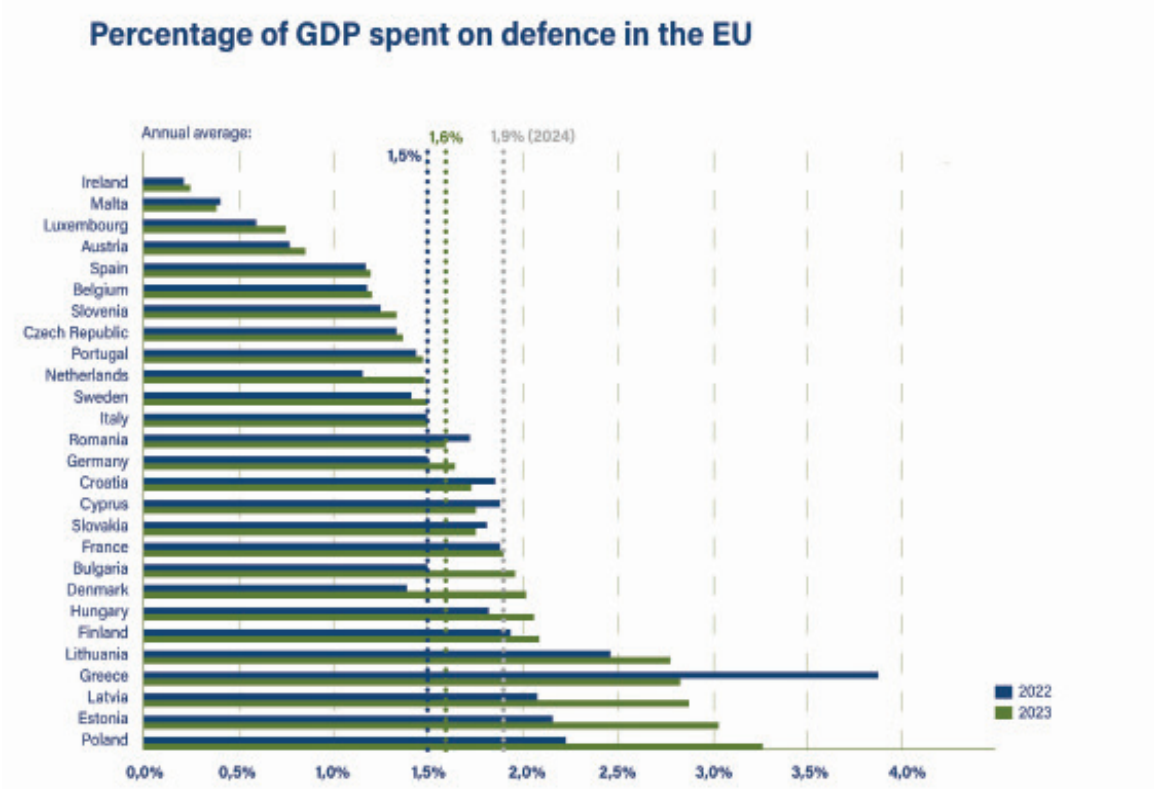
Overall government spending on defence in the EU (2022-2023)

To get a picture of the expected growth in maritime defence for the coming years and decades, an assessment of current and projected defence spending in general is important.

Based on the recent evolution, public spending on defence has been growing rapidly in recent years and is expected to continue rising. In the European Union, defence spending has increased from 1.5% of GDP in 2022 to 1.9% in 2024. By comparison, the United States spent 3.4% of its GDP on defence in 2023.

Over the next two years, EU defence budgets are likely to rise significantly, particularly as countries that have traditionally spent less—such as Ireland, Spain, and Belgium—begin to catch up. Looking ahead to 2030, it is expected that the average defence spending in the EU could exceed 3% of GDP.

In the case of Belgium, this implies more than doubling its annual defence spending and investments.

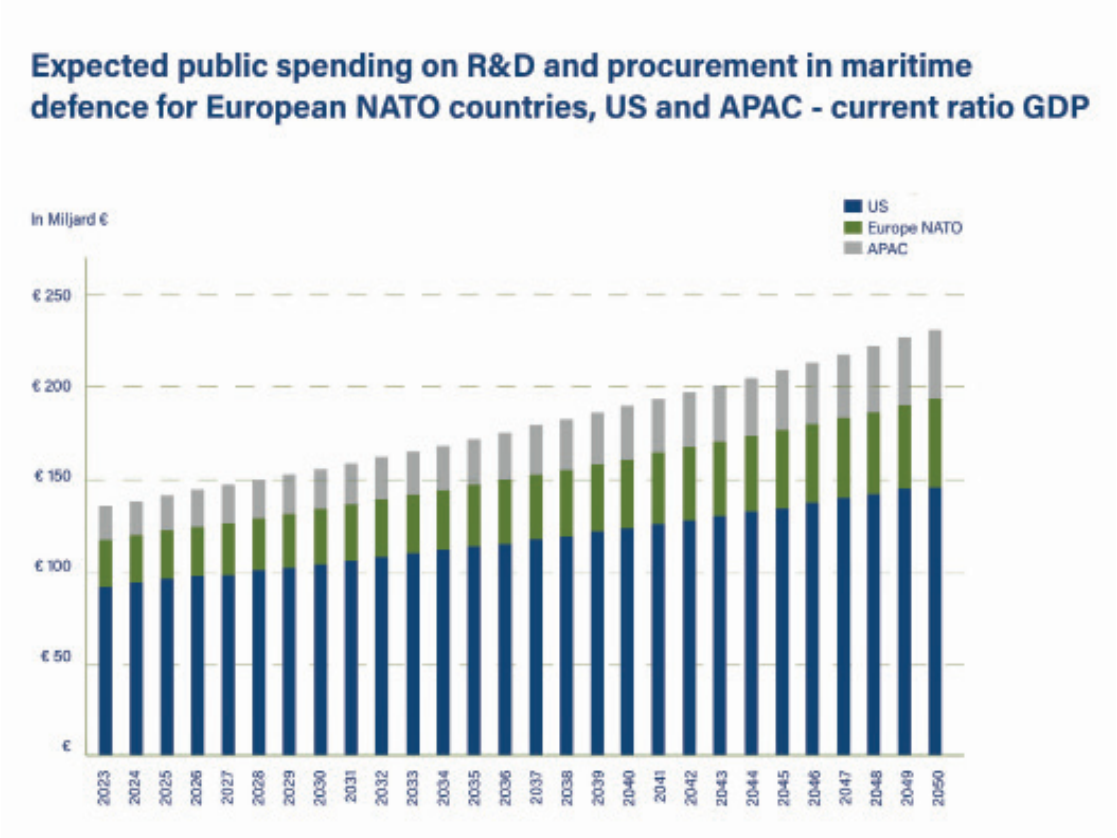


Global government spending on maritime defence (2023-2050)

To gain insight into global maritime defence spending, the analysis begins with the total national defence expenditures of countries in three key regions: EU NATO, APAC, and the United States. This total is then refined to estimate the share allocated specifically to maritime defence, focusing on procurement and R&D.

This breakdown serves as a proxy for identifying the upper limit of investment potential in maritime security technologies. In other words, it reflects the maximum pool of resources that could, directly or indirectly, be available for innovation, partnerships, and supply chain involvement in this domain.

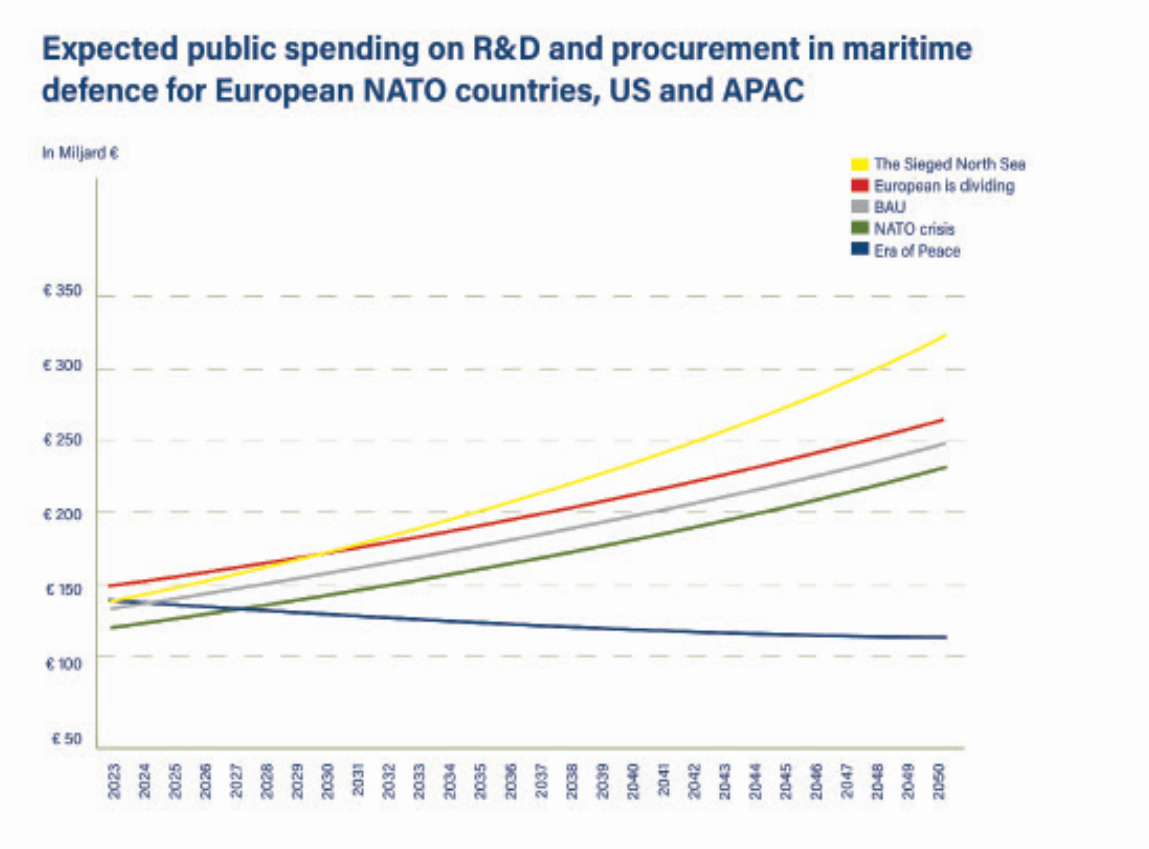
For Belgian companies, this provides strategic insight into where market opportunities may emerge. It highlights not only the scale of potential demand for maritime technologies—such as naval systems, underwater surveillance, shipbuilding innovations, and cybersecurity for maritime infrastructure—but also which regions and stakeholders are most likely to drive that demand.



Foresight Government spending on Maritime defence (2023-2050)

By calculating the variation in key input variables—such as defence spending as a percentage of GDP, the share allocated to maritime defence, and regional potential in Europe and the US—across the 4 defined scenarios, a clear conclusion emerges: in three out of four scenarios, public spending on maritime defence is expected to grow significantly.

According to the projections, this spending is expected to at least double between now and 2050, with estimated values ranging between €240 million and €325 billion, depending on the scenario. This reflects a substantial long-term investment trend, reinforcing the strategic importance of maritime defence and growing opportunities for companies active in this domain.



© **Blue Cluster,** October 2025.

This publication would not have been possible without the valuable input, expertise and engagement of the companies, research institutions and public authorities within Blue Cluster's network. We sincerely thank you for your time, openness and input for this document.

Authors:
Eveline Buyck; Arnout Desmet; Frank Gielen; and Piet Opstaele.

Please refer to this publication as follows:
Blue Cluster (2025). Feasibility Study: Ecosystem development for critical maritime infrastructure protection.

Blauwe Cluster vzw
Bluebridge
Wetenschapspark 1
B-8400 Oostende

T +32 (0)50 26 75 15
www.blauwecluster.be