BLUE CLUSTER

ORIENTATION ROADMAP

Maritime Security and Defence Systems

MARCH 2026

COMMISSIONED BY

WEWIS
Department of Work
Economy, Science
Innovation & Social Economy

Contents

1 Vision and context 2

2 Flanders, a breeding ground for maritime innovation 4
- 2.1 Fixed surveillance 5
- 2.2 Drones 5
- 2.3 Automated systems and robotics 6
- 2.4 Communication systems 6
- 2.5 Data analytics and artificial intelligence 7

3 Orientation Roadmap for Maritime Defence 8
- 3.1. Deter: discouraging and preventing hostile presence and actions 9
- 3.2. Detect & Identify: early recognition of threats below, on, and above the water 10
- 3.3. Respond: coordinated response to detected threats or hostile actions 10
- 3.4 Repair: restoration of systems, infrastructure, and operational capacity 11

4 Innovation opportunities 12
- 4.1. Fixed surveillance 12
- 4.2. Drones and autonomous vehicles (UAVs, USVs and UUVs) 13
- 4.3. Automated systems and robotics 14
- 4.4 Communication systems and connectivity 15
- 4.5 Data analytics and artificial intelligence 16
- 4.6 Cybersecurity 17
- 4.7 Collaboration 18

5 Conclusion 19

1. Vision and context

The maritime domain is rapidly evolving worldwide into a strategic space where economic, security, and technological interests converge. While maritime areas were once primarily trade routes and energy corridors, they have now also become the frontline of geopolitical tensions and technological competition. Infrastructure on and beneath the sea, data networks, and maritime logistics are no longer merely civilian assets, but vital components of national and European security.

The recent increase in incidents at sea highlights the vulnerability of these infrastructures to sabotage, espionage, and unwanted reconnaissance activities. The mapping of critical infrastructure and the deployment of autonomous, unmanned vessels further add to the complexity of the threat landscape. At the same time, the growing digitalisation of maritime systems - from ship navigation to offshore control platforms - introduces new risks.

Against this backdrop, the need for a stronger and future-oriented maritime defence industry is growing. Flanders is exceptionally well positioned to take on this role. It has a strong maritime and technological ecosystem in which industry, knowledge institutions, ports, and defence actors reinforce one another. This ecosystem brings together critical infrastructures - from logistics and energy to data communication and offshore technology - making Flanders particularly suited to develop, test, and valorise new maritime defence technologies.

A forward-looking maritime defence strategy should build on this by focusing on:

- **Strengthening defence expertise**: Flanders is a frontrunner in autonomous underwater systems and mine countermeasure capabilities, areas in which it plays a leading role both nationally and internationally..
- **Protecting vital and critical infrastructure**: Offshore energy, data cables, pipelines, and logistics hubs require advanced monitoring, digital security, and rapid response capabilities..
- **Cybersecurity and digital resilience**: The digitalisation of maritime systems requires advanced threat detection, secure communication, and robust data infrastructures..
- **Interoperability and collaboration**: Effective cooperation between civilian, military, and private actors requires open standards, shared situational awareness, and innovative ecosystems.

In addition to Flemish ambitions, this strengthening aligns closely with the broader European security framework, as outlined in the *White Paper for European Defence – Readiness 2030*. The European Union recognises the strategic importance of the maritime domain as a vital component of its defence and resilience strategy. Key priorities include the protection of subsea infrastructure, enhanced maritime situational awareness, and interoperability within a NATO context.

The European Union also explicitly links its ambitions in maritime security and defence to strengthening the **European Defence Technological and Industrial Base (EDTIB)**. It recognises that strategic autonomy in the maritime domain depends not only on military capabilities, but also on a robust industrial base that is innovative, interoperable, and less dependent on third countries.

Within this European agenda, the following priorities emerge:

Protection of critical maritime infrastructure: Europe recognises a growing threat of sabotage targeting pipelines, data cables, and offshore installations. The North Sea is explicitly identified as a vulnerable region for hybrid threats. Efforts focus on enhanced subsea surveillance, electronic protection, and faster response mechanisms.

Maritime Domain Awareness (MDA): The EU aims to strengthen the maritime picture through the integration of data from air, surface, and underwater sensors, supported by AI and satellite technologies. This closely aligns with Flemish initiatives in sensor fusion and digital twins.

Military mobility and dual-use infrastructure: The European Commission identifies maritime logistics hubs, such as ports, as essential links for military mobility. Investments in robust, interoperable, and secure port capacity are considered a priority. Flemish industrial players can play a key role by providing technologies that support both civilian and military applications..

Autonomous systems and maritime robotics: The EU promotes joint research and development in areas such as unmanned vessels (UUVs, USVs), mine countermeasures, and underwater exploration - technologies in which Flanders already takes a leading position and where further synergies can be developed with European programmes such as the European Defence Fund (EDF) and PESCO projects.

Cyber and electronic warfare: Given the increasing digitalisation of maritime systems, strong emphasis is placed on cyber resilience and the protection of the electromagnetic spectrum, including for maritime and subsea assets. This aligns with the Flemish focus on AI-driven cyber detection and end-to-end security architectures.

Public-private collaboration and innovation: The EU considers maritime security a strategic sector in which innovative SMEs and knowledge institutions play a key role. Thanks to its strong technological base and industrial maturity, Flanders can act as a proactive partner in pan-European defence ecosystems.

With this roadmap, Flanders positions itself as a **proactive industrial and technological partner** within European and NATO initiatives on maritime security, surveillance, and hybrid threat detection in the Greater North Sea Basin. The further sensorification of the North Sea - from subsea sensors to UAV-based observation systems - contributes to NATO's objective of Full Ocean Space Situational Awareness and strengthens Flanders' role in the development of dual-use technologies.

Flemish ports also support this ambition as facilitators of innovation and collaboration. They act as industrial and logistical hubs within European military mobility corridors, thereby contributing to the resilience of these corridors. The development of a strong defence industry not only supports military capability building, but also strengthens Flanders' economic and technological position within Europe. NATO likewise emphasises the importance of "layered resilience", in which industrial innovation and security reinforce one another.

2. Flanders, a breeding ground for maritime innovation

The Flemish ecosystem for maritime security and defence is diverse and rapidly evolving. It builds on a strong foundation of government and naval support, combined with close collaboration between research institutions and innovative companies. The interaction between knowledge institutions and SMEs, in particular, acts as a key driver of innovation. Flanders develops technological solutions that enable both defence-specific applications and dual-use technologies, with applications in ports, offshore energy, and maritime security and defence.

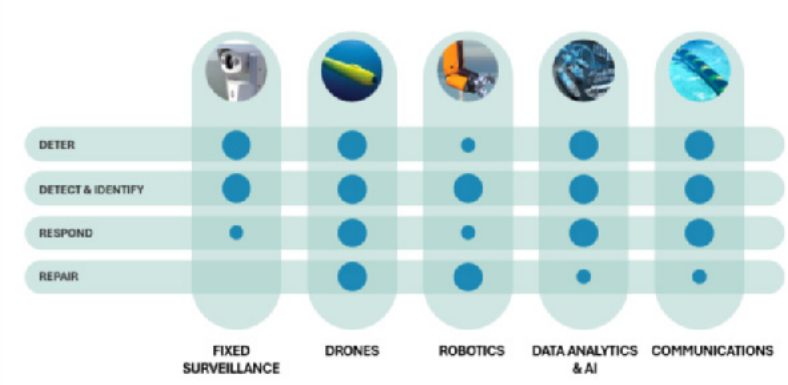
Within the Flemish maritime defence ecosystem, clear areas of strength are emerging. Flanders has reached a c**ritical mass** in specific domains where expertise, industry, and international collaboration are already well developed, alongside several **growth areas** where further consolidation and scaling are needed.

Flanders ranks among Europe's leaders in **mine countermeasures (MCM)** and **autonomous underwater systems**. The combination of technological innovation, operational expertise, and collaboration with the Belgian Navy has positioned Flanders as an internationally recognised frontrunner in underwater drones, mine detection, and mine clearance. This expertise provides an important gateway to European and NATO programmes.

In domains such as **AI-driven data fusion**, **maritime cybersecurity**, **automated maritime systems**, and **sensor integration**, Flanders is strong in knowledge development and pilot projects. At the same time, further industrialisation and clustering are needed to secure a sustainable market position. Initiatives such as test zones in port environments and joint research projects with defence can help accelerate this growth.

Flanders is also building emerging strengths in **predictive AI applications**, **digital twins**, **sensor networks**, and **dual-use robotics**. These niches hold strong innovation potential and can evolve into technological specialisations.

To make this innovative potential more tangible, the Flemish maritime defence ecosystem can be divided into several **core technological domains**. Each of these domains represents a crucial link within the broader maritime security landscape, while also reflecting the strong knowledge base and industrial capabilities that Flanders currently possesses. Together, they form the foundation on which Flanders can further develop its role as a leading player in maritime security, defence, and dual-use technologies.



2.1 Fixed surveillance

Systems designed to **monitor** or **detect** activities within a defined area, using **passive or active techniques**. These installations are stationary and do not have autonomous response capabilities.

Some examples:

Subsea Surveillance Systems: Permanent or semi-permanent systems deployed on the seabed or within the water column to detect, track, and classify underwater objects or activities. They use technologies such as active and passive sonar, distributed acoustic sensing (DAS), magnetic anomaly detectors, and more.

Application: monitoring critical subsea infrastructure and detecting underwater threats (such as divers or unmanned underwater drones).

Surface & Air Surveillance Systems: Fixed systems installed on land, offshore installations, or platforms to monitor surface vessels and other objects. They use technologies such as coastal and offshore radars, fixed cameras (including 360°), satellite monitoring, drone detection sensors, and AIS-based systems.

Application: detecting and tracking vessels and objects on and above the water, enabling visual monitoring, and enhancing situational awareness around strategic infrastructure.

2.2 Drones

Mobile robotic systems that operate **autonomously** or **semi-autonomously** in air, surface, and underwater environments. They collect data, perform monitoring tasks, or carry out specific operations on site. **Mobility** is the core function, in contrast to fixed installations.

Some examples:

Unmanned Aerial Vehicles (UAVs): Remotely operated or autonomous aerial systems that operate without a pilot on board (in various forms such as fixed-wing - long range and large payloads - and rotary-wing, offering VTOL capabilities and precision).

Application: intelligence, surveillance and reconnaissance (ISR), air surveillance, maritime patrols, military operations.

Unmanned Surface Vehicles (USVs): Autonomous or semi-autonomous vessels that operate on or near the sea surface without onboard crew. They use advanced navigation, sensors, communication systems, and efficient propulsion.

Application: intelligence gathering, mine detection and clearance, anti-submarine operations, resupply, direct deployment, and data transmission.

Autonomous Underwater Vehicles (AUVs): Unmanned underwater robots that perform missions independently. They are equipped with navigation systems, sonar, optical cameras, and sensors, and often require complex communication solutions.

Application: inspection of subsea infrastructure, detection and neutralisation of threats, and underwater search operations.

2.3 Automated systems and robotics

Autonomous or semi-autonomous physical systems embedded in or connected to infrastructure. They perform **predefined or AI-driven actions** in response to external stimuli.

Some examples:

Onboard Control & Operational Systems: Automated systems integrated into vessels or fixed maritime installations to manage and optimise core operations. This includes, among others, autopilots, dynamic positioning systems, and integrated bridge functions.

Application: improving efficiency, safety, and performance; reducing human intervention; optimising operational reliability.

Integrated Safety & Security Systems: Automation systems designed to monitor, detect, and respond to safety risks and security breaches within maritime infrastructures. Examples include detection systems, access control, emergency response, and screening technologies.

Application: providing real-time alerts and automated countermeasures; strengthening physical safety and protection against threats.

2.4 Communication systems

Technologies that enable the **transmission, routing, and integrity of data, commands, or alerts** between physical and digital components.

Some examples:

Operational Technology (OT) Networks: Networks and systems that control physical processes and devices within maritime operations. These include SCADA systems, propulsion and machinery management, navigation systems (GPS, ECDIS, radar), bridge systems, and safety networks such as HVAC and fire detection.

Application: direct control of vessel and port operations; essential for cyber-physical security and operational continuity.

Information Technology (IT) Networks: Networks and systems focused on data processing, information management, and administrative functions. Examples include cargo and environmental management systems, access and screening solutions, crew and welfare applications, and shore-to-ship data exchange.

Application: supporting administrative, logistical, and operational processes, and enabling secure data exchange between systems.

External Communication Systems: Infrastructures and protocols that enable communication between maritime assets and external entities. This includes satellite communication (Satcom), maritime radio links (GMDSS), 5G nodes, subsea cable repeaters, AIS, and GNSS/GPS.

Application: ensuring data transmission, command communication, and the dissemination of alerts across the maritime domain.

2.5 Data analytics and artificial intelligence

Software and systems that **analyse** and **interpret** collected data, and **generate predictions** - such as pattern recognition, threat classification, behavioural modelling, and operational optimisation.

Some examples:

Threat Detection & Anomaly Identification: AI and machine learning models identify anomalies, suspicious patterns, or unauthorised activities in maritime data. They use techniques such as machine learning, deep learning, and reinforcement learning.

Application: real-time detection of intrusions, navigation anomalies, unauthorised access, and irregular data transmissions.

Predictive Analytics & Risk Assessment: AI-driven systems analyse data to predict threats or operational issues at an early stage and assess risks. Techniques include deep learning, natural language processing (NLP), and graph-based AI.

Application: predictive maintenance, maritime threat analysis, cyber risk assessment for autonomous vessels, and forecasting of cyberattacks.

Data Integration & Situational Awareness: Advanced AI/ML platforms combine data from multiple sources into a unified operational picture used for situational awareness and decision-making. Techniques such as federated learning and blockchain-enhanced AI improve data security and reliability.

Application: multisource data synthesis, secure data exchange, privacy-preserving analytics, and enhanced visibility of the maritime domain.

3. Orientation Roadmap for Maritime Defence

Maritime defence is approached within this framework through the **DDIRR principle**: Deter, Detect, Identify, Respond & Repair. This model provides a strategic structure to manage a wide range of threats in the maritime domain, ranging from cyberattacks to underwater infiltrations, mine-laying activities, sabotage operations, and conventional military threats.

This principle applies to both **civil-military infrastructure** (such as ports, offshore wind farms, and data cables) and **military operations** (such as naval defence and mine countermeasures).

The integration of a recovery component ("Repair") is essential to ensure long-term resilience in a highly dynamic environment.

MARITIME SECURITY

DETER	DETECT & IDENTIFY	RESPOND & REPAIR
Discouraging access	***Early detection of anomalies and suspicious activities above, on and below the water***	***Rapid and coordinated deployment of assets in case of incidents or conflict situations, rapid repair following incidents***
Preventing unauthorized or hostile access to systems, infrastructure and strategic zones in both civilian and military contexts. Conceptual, physical and digital. • Continuous patrol and perimeter enforcement (surface, air, underwater) – mix of platforms; need for integrated sensors in air, surface and underwater domains to avoid blind zones. • Deterrence through visible and invisible presence (autonomous systems and surveillance) by strengthening physical and digital barriers. • Digital defensive capabilities against spoofing, jamming and data manipulation become critical. Establishing resilient, robust IT & OT systems with redundancy.	• Detection: Multidimensional detection of threats below, on and above water through fixed and mobile sensors (radar, sonar, drones, underwater robotics), including detection of digital sabotage or electromagnetic interference. • Identification: Sensor fusion and AI-based pattern recognition are crucial for early and autonomous identification of anomalous behaviour, objects and digital threats (data from combined sensor networks (radar, lidar, sonar, cameras, ...), AI-driven pattern recognition, interoperable systems). • Data integration across civilian, industrial and military sensor networks, with AI models trained on tactically relevant anomalies. • Optimising underwater detection by reducing acoustic noise and deploying mobile sensors. • Intelligence sharing to improve situational awareness and shorten response times.	• Readiness: Rapidly deployable (autonomous) response assets (drones, UUVs, robotics) for tactical actions such as mine detection, interception or response to sabotage. • Execution: Improved coordination between autonomous systems in air, surface and underwater domains (swarm operations). • AI-supported command and control and real-time data fusion (human–machine teaming and multi-agent operations in complex threat scenarios). • Repair: Mobile repair capabilities at sea (e.g. autonomous inspection and repair robots), redundant infrastructure and digital resilience for critical systems. • Cybersecurity: Detection of and recovery from attacks (e.g. spoofing, data manipulation), security-by-design and failover mechanisms. • Civil–military coordination and communication, and interoperable protocols (uniform analysis and interpretation) for rapid response and repair.

3.1 Deter - discouraging and preventing hostile presence and actions

Deter focuses on **discouraging** access to maritime zones or systems by establishing conceptual, physical, and digital barriers. This includes a **persistent presence** through unmanned patrol systems, detection networks securing subsea areas, and digital infrastructure resilient to sabotage or intrusion. Both the deployment of visible capabilities and strong **cyber resilience** are essential. Deter also implies demonstrating the **capacity** and **willingness** to take countermeasures if our interests are threatened.

Capability gaps & needs:

Permanent situational awareness: continuous monitoring of maritime zones through subsea and surface patrols, unmanned vessels (USVs, AUVs), and integrated sensor networks. Flemish companies and knowledge institutions are developing technologies for real-time detection, identification, and threat analysis that can be directly deployed in military operations or as part of collective defence.

Protection and reinforcement of maritime infrastructure: development of detection and protection systems for subsea cables, energy connections, pipelines, and port networks. Flemish actors contribute to defence needs through **subsea surveillance systems**, **intrusion detection**, **digital barrier technologies**, and **autonomous inspection systems**.

Digital and cyber resilience: Strengthening maritime OT and IT systems against sabotage and cyber intrusion through AI-driven threat detection, secure communication, and resilient data infrastructures. These technologies have both civilian and military relevance and are essential for securing command-and-control systems.

The industrial applications within these pillars directly support concrete defence capabilities. They contribute to maritime intelligence, surveillance and reconnaissance (ISR), the protection of NATO- and EU-supporting infrastructure, and underwater domain protection.

3.2 Detect & Identify – early recognition of threats below, on, and above the water

This phase focuses on **detecting** and **identifying** abnormal movements, behaviour, or objects that may indicate a threat. These can include mines, unmanned (hostile) vessels, cyberattacks, or suspicious patterns in maritime traffic.

Identification requires sensor fusion, AI-driven pattern recognition, and interoperable systems capable of operating across **three dimensions**: above, on, and below the water.

Capability gaps & needs:

- Insufficient data integration between civilian/industrial and military sensor networks.
- AI systems are not yet sufficiently trained for automatic identification of tactically relevant targets in this complex maritime environment.
- Underwater detection is limited by acoustic constraints and a lack of mobile sensors.
- Detection of digital sabotage or electromagnetic interference requires further development.

3.3 Respond – coordinated response to detected threats or hostile actions

The response phase focuses on the **rapid** deployment of assets following detection. This includes neutralising mines, intercepting hostile UUVs, or securing damaged installations. In a hybrid context, this also involves civil-military coordination and restoring control over systems after a cyberattack.

Capability gaps & needs:

- Insufficient flexible and deployable response capacity.
- Limited swarm coordination between autonomous platforms operating below, on, and above the water.
- Real-time communication remains vulnerable in jamming environments or when satellite navigation is disrupted.
- Decision-making tools are not sufficiently adapted to multi-agent operations in complex threat scenarios.

3.4 Repair – restoration of systems, infrastructure, and operational capacity

Repair is a critical component within maritime defence: following an attack, explosion, failure, or sabotage, systems, infrastructure, and networks must be **restored** quickly to remain operational or become deployable again. This includes not only **physical** repair (e.g. damage to vessels, cables, buoys, platforms), but also the functional recovery of **digital** systems and sensor networks.

Capability gaps & needs:

- There is a lack of mobile repair capacity at sea: autonomous or robotic systems capable of assessing and mitigating damage locally.
- Subsea infrastructure (e.g. cables, sensors) is difficult to access and slow to repair without advanced UUVs and intervention robots.
- Digital systems are often not designed with resilience in mind: there is a need for redundancy, automatic isolation, and fallback systems in case of cyber intrusions or breaches of digital systems.



4. Innovation opportunities

4.1 Fixed surveillance

Within fixed surveillance systems, innovation opportunities lie in multimodal detection, where, for example, offshore radar installations, smart buoys at the water surface, and underwater sonar fields operate together as a single sensory ecosystem. AI-driven pattern recognition enables these systems to detect anomalies at an early stage, whether originating from suspicious vessels at the surface, low-flying objects in the air, or underwater activity such as divers or UUVs.

Through sensor fusion and digital twins, data from these three layers - for example, visual cameras on vessels, hydrophones on the seabed, and air traffic monitoring via UAVs - can be integrated into a real-time operational picture. This not only allows for the detection of current threats but also enables predictions of potential incidents or damage. This approach supports both the protection of civilian infrastructure such as offshore wind farms and the early detection of hostile underwater activity in a military context.

Innovation opportunities:

- Combination of different monitoring systems:
  - Air: radar installations, aerial cameras, air traffic monitoring, ...
  - Surface: maritime radars, visual cameras, smart buoys, ...
  - Underwater: sonar fields, hydrophones, seabed sensors, ...
- Multimodal detection using AI-driven pattern recognition and automatic anomaly detection.
- Sensor fusion and digital twins for real-time situational awareness, including prediction of threats and damage.
- Protection of critical infrastructure (wind farms, data cables, terminals) as well as deployment for early detection of hostile underwater activity and mine detection.

4.2 Drones and autonomous vessels (UAVs, USVs, UUVs)

Autonomous vessels and drones represent a new generation of operational assets capable of covering the maritime domain across three dimensions: in the air (UAVs), on the water (USVs), and underwater (UUVs). These platforms operate independently and are designed to carry out reconnaissance, surveillance, and response missions, often without direct human intervention. Their added value lies in their mobility, flexibility, and ability to operate in combination, where multiple platforms coordinate in so-called "swarm operations." For example, a UAV can monitor an area from the air, while a USV patrols the surface and a UUV simultaneously conducts subsea inspections or detects mines.

Within this domain, the focus is on developing systems that can plan missions, respond to changing conditions, and collaborate with other vessels using artificial intelligence. The reliability of navigation and communication systems is crucial, especially in environments where GPS disruption or electronic countermeasures (such as spoofing or jamming) may occur. Through redundant technologies - such as combining visual recognition with magnetic or inertial references - these autonomous systems can continue to operate effectively.

Autonomous vessels and drones are particularly suited for tasks where range, speed, and coordination are essential. They provide situational awareness in complex or hybrid threat scenarios and can respond rapidly to emerging events. Within a maritime defence strategy, they form a flexible and deployable layer capable of detecting threats at an early stage and, if necessary, neutralising them autonomously.

These systems are also of strategic importance for mine countermeasures, where UUVs are deployed to detect, classify, and neutralise sea mines in complex operational environments.

Three-dimensional deployment:

- UAVs: above water - reconnaissance, patrol, inspection, logistics
- USVs: on the water - perimeter surveillance, mine detection, response platform
- UUVs: underwater - inspection, mine countermeasures, reconnaissance, and combat support

Innovation opportunities:

- Fully autonomous systems: vessels and drones that use AI for mission planning, navigation, and adaptive response without continuous human intervention.
- Integrated maritime threat picture: combining multi-platform sensor input (air, surface, underwater) into a single decision-making model for a coherent operational picture.
- Cyber and signal resilience: protection against spoofing and jamming through redundant methods (visual, inertial, magnetic).
- Autonomous collaboration (swarming): coordination and joint operations of multiple unmanned systems above, on, and below the water.
- Dual-use sensor technology: Flemish expertise in miniaturisation and sensor fusion applicable to both civilian use (e.g. inspection drones) and maritime defence (UUVs).
- Manned-Unmanned Teaming: integration of crewed platforms (e.g. frigates) with USVs and UUVs for combined maritime operations.
- Sustainable energy and propulsion: innovations in battery and fuel cell technologies enabling longer mission duration and greater operational autonomy.

4.3 Automated systems and robotics

Automated systems and robotics focus on strengthening maritime security and defence by automating detection, surveillance, and response processes within and around infrastructure. These systems operate continuously or in standby mode and are automatically activated in response to suspicious activity or sabotage attempts.

The core of this domain lies in the integration of sensors, decision logic, and communication into a single system, minimising human intervention and significantly increasing response speed. Automated systems can perform perimeter surveillance, detect suspicious movements, and initiate an initial response. They are designed to quickly isolate incidents and transmit information in real time to higher levels of command.

In the field of underwater robotics in particular, this domain enables the execution of high-risk, precision tasks in hard-to-reach or hostile environments. This includes inspecting and identifying suspicious objects underwater, as well as neutralising explosives and mines in a controlled and safe manner. These robotic systems are particularly suited to environments where manual intervention would be too slow or too dangerous.

In addition to detection and response, such systems can also be deployed for post-incident repair and stabilisation tasks, such as restoring damaged sensors, infrastructure, or communication links in difficult-to-access areas.

Innovation opportunities:

- Automated response mechanisms integrated into maritime infrastructure
- Underwater robotics for precision tasks such as inspection, detection of hostile objects, and targeted neutralisation of explosives or mines in controlled operations
- Deployment of robotics in hostile or unpredictable environments where manual intervention is too risky

4.4 Communication and connectivity

Effective maritime security depends on the ability of all systems - in the air, on the water, and underwater - to communicate securely and reliably with one another. Connectivity is equally important, for example through the use of shared protocols and the ability to analyse and interpret data in a uniform way. Aerial drones (UAVs) can, for instance, temporarily act as relay nodes, enabling information to be transmitted via wireless networks or satellite directly to a control centre. On the water, 5G can ensure that vessels and infrastructure remain connected. Underwater, UUVs and fixed sensors can use acoustic or optical signals to exchange data.

It is essential to invest in redundant and resilient networks that continue to function in the presence of spoofing and jamming attempts. Secure system integration is also critical, allowing, for example, a UAV detecting a suspicious situation to immediately transmit that information to an underwater drone preparing for action. The objective is to create a seamless and secure data network in which all systems operate together, regardless of their location.

An additional challenge lies in the development and implementation of interoperable protocols and common standards. Only when systems "speak the same language" can information from different networks and sensors be presented and interpreted in a consistent and reliable way. This not only facilitates cooperation but also improves the efficiency and speed of decision-making.

Innovation opportunities:

- Need for secure and interoperable communication across three dimensions:
    - Air/surface: robust, redundant networks (such as offshore 5G, mesh networks, and satellite links) ensuring continuous connectivity between drones, vessels, and infrastructure.
    - Underwater: acoustic, optical, or electromagnetic communication with UUVs and fixed sensors for reliable data transmission in GPS-denied environments.
    - Spoofing- and jamming-resistant communication systems capable of autonomously switching between connection types in case of disruption or hostile interference.
    - Secure interoperability between maritime platforms, drones, sensor networks, and control centres across all dimensions.
    - Real-time data sharing between unmanned systems and command structures to enable coordinated actions in detection, reconnaissance, and response.
    - Development and implementation of common standards and protocols, allowing data from diverse networks and sensors to be integrated and utilised in a consistent and reliable manner.

4.5 Data analytics and artificial intelligence

AI technologies are essential for rapidly processing information from multiple sources - such as aerial imagery, radar, sonar, and underwater sensors - into a coherent operational picture. By intelligently combining large volumes of data, AI can identify anomalous patterns that would otherwise go unnoticed. For example, detecting unusual underwater movements shortly after a suspicious drone has landed nearby.

Using predictive algorithms, AI can also identify trends, such as repeated navigation routes around sensitive infrastructure or subtle changes in underwater acoustics that may indicate mine-laying or sabotage activities.

AI supports operational decision-making by providing targeted analyses and recommendations, while leaving final actions to human operators or predefined command structures.

Innovation opportunities:

- AI-driven detection of cyber threats and anomalous behaviour in maritime networks, based on continuous monitoring
- Advanced data fusion from air, surface, and underwater sensors to create a coherent, real-time operational picture
- AI-supported decision-making, where systems provide recommendations based on pattern recognition and risk assessment - without autonomous intervention
- Predictive AI models that analyse trends and identify potential risks and incidents

4.6 Cybersecurity

Modern maritime operations increasingly depend on digital systems for navigation, communication, detection, and coordination. This digitalisation increases vulnerability to cyberattacks aimed at disrupting data flows, taking control of systems, or manipulating sensor data. Autonomous vessels and connected infrastructure are particularly at risk when their software, connections, or decision-making processes are disrupted or deceived. Cybersecurity has therefore become a fundamental requirement for the safe deployment of maritime technologies.

It is essential to invest in digital redundancy and failover architectures that can automatically take over critical functions in case of disruption or manipulation, ensuring that systems remain operational during and after an attack.

- Protection of connected sensors, drones, and infrastructure against manipulation, sabotage, or data breaches
- Protection of critical systems against cyberattacks targeting communication, navigation, or decision-making
- Real-time detection of digital intrusions, both onboard vessels and in control centres

Cybersecurity is an integral part of maritime security. Critical maritime infrastructures - ports, offshore wind farms, data cables, and vessels - are increasingly becoming digital ecosystems. The Cybersecurity for Defence roadmap highlights how cyberattacks and hybrid warfare directly impact both military operations and civilian infrastructure. This maritime roadmap aligns closely with that framework: while the cyber roadmap focuses on generic OT and IT security, this maritime roadmap translates that framework into concrete applications in the North Sea region and Flemish ports.

More specifically, protecting the maritime domain - from both a civilian and dual-use perspective - aligns closely with the FORTIFY (security-by-design) and SHIELD (operational security) pillars of the Cybersecurity for Defence roadmap. In addition, the CONTROL pillar focuses on specific cybersecurity technologies supporting cyber defence operations, including maritime operations.

Innovation opportunities:

- AI-driven threat detection: automatic identification of cyberattacks through anomaly detection in network traffic and data flows
- Cyber control in command structures: integration of cyber alerts and automatic isolation of affected components within maritime C2 processes
- Cyber resilience of systems: increased resilience of autonomous platforms and maritime OT/IT systems against sabotage, spoofing, and malware
- Interoperable security architectures: end-to-end protection of communication between drones, infrastructure, and command centres
- Secure-by-design technology: embedded hardware and software security from the concept phase in drones, sensors, and platforms
- Quantum-secure communication: application of post-quantum cryptography in satellite and offshore networks
- Threat intelligence sharing: maritime SOCs and ports as testbeds for active information exchange on threats
- Digital twin security: integration of cybersecurity into maritime digital twins to safely simulate scenarios and risks

4.7 Collaboration

Collaboration between stakeholders is a key pillar in the further development of the Flemish maritime defence industry. Given the cross-border nature of the maritime sector, particularly with regard to offshore installations and ports, it is crucial to foster cooperation between public and private actors, international partners, and maritime security experts.

This collaboration should focus on enabling technology integration, improving coordination, and ensuring open data exchange. This allows systems to be seamlessly aligned, threats to be shared more rapidly, and response operations to be carried out more effectively. International cooperation is also essential for organising joint patrols and developing common emergency response strategies.



5. Conclusion

The Flemish North Sea and ports are evolving into strategic hubs at the intersection of energy supply, digital infrastructure, and international logistics. At the same time, their vulnerability is increasing in a context of rising geopolitical tensions and hybrid threats. This reality highlights the need for a structural and forward-looking approach to maritime security and defence.

With the Security and Defence Impulse Programme, the Flemish government is taking an important step towards building a robust, innovative, and internationally anchored technological and industrial defence base.

This programme is not limited to the protection of critical maritime infrastructure such as offshore wind farms, data cables, and ports, but also covers broader defence applications such as naval combat, underwater defence, and mine countermeasures (MCM) - domains in which Flanders already plays a recognised leading role.

The resulting roadmap provides companies, knowledge institutions, and public authorities with a concrete and integrated framework to collaborate on key technologies such as AI, autonomous systems, underwater robotics, cybersecurity, sensor fusion, and digital decision-making. By combining civilian and military applications (dual-use innovation) and strengthening public-private cooperation, a dynamic ecosystem is created that responds to the strategic needs of today and tomorrow.

This Impulse Programme contributes to the resilience of Flanders and Belgium, supports European technological autonomy, and strengthens our role as a reliable partner within NATO and the European Union. This maritime roadmap forms the foundation on which future projects can be built - as a lever for innovation, security, and economic growth.

© **Blue Cluster,** March 2026.

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

Authors:
Eveline Buyck (ed.).

Please cite this publication as follows:
Blue Cluster (2026). Orientation Roadmap for Maritime Security and Defence Systems.

De Blauwe Cluster
Bluebridge
Wetenschapspark 1
8400 Oostende
Belgium

T +32 50 26 75 15