Call for proposals

RESEARCH 2026-2

Information document including submission and evaluation guidelines and budget rules
For more information on the programme, please visit
https://www.bluecluster.be/blue-bastion

Important dates:

- Information day: Wednesday 26 August (10h00 - 12h00)
- Deadline pre-proposals: Thursday 1 October 2026 (23h59)
- Deadline full proposals: Tuesday 1 December 2026 (23h59)
- Start date projects: Monday 4 January 2027
- End date project: Monday 5 July 2027

SUMMARY

The RHID & Blue Cluster **Blue Bastion Research Call 2026-2** supports applied research and technology development for the protection of critical maritime infrastructure, with a strong focus on collaborative research consortia bringing together industry, knowledge institutions and operational stakeholders.

This call supports research projects with a maximum duration of **24 months** and funding of up to **EUR 2,000,000 per project,** targeting the development, validation and maturation of innovative concepts, technologies and prototypes in the **TRL 3–5** range.

- The call fosters an **ecosystem** in which industry, knowledge institutions and operational stakeholders collaborate to address strategic maritime security challenges through multidisciplinary research and innovation.
- Projects must align with the Blue Cluster Maritime Security Roadmap and contribute to future capability development, technological maturity and protection of critical maritime infrastructure.
- The call focuses on two priority research domains: **Integrated Detection, Attribution & Response for Underwater Threats and Next-Generation Protection & Resilience of Critical Maritime Infrastructure.**
- Research projects are expected **to generate new scientific knowledge**, validated technologies, prototypes or system concepts, providing a clear pathway towards future demonstrator projects, operational validation and **European collaboration opportunities**.
- The call contributes to the development of **a strong Belgian knowledge, industrial and technology base in maritime security and critical infrastructure** protection, while supporting future participation in European defence, security and maritime innovation programmes.
- The deadline for submitting the pre-proposals is **1 October 2026**, for the full proposals **1 December 2026**, with project start dates on 1 April 2027 and an end date of **31 March 2029**.

TABLE OF CONTENTS

SUMMARY 2
TABLE OF CONTENTS 3
1. RESEARCH, DEVELOPMENT, INNOVATION AND INDUSTRIALIZATION OF THE MINISTRY OF DEFENCE 6
1.1. CONTEXT 6
1.2. ROLE OF THE ROYAL HIGHER INSTITUTE FOR DEFENCE - RHID 6
1.3. BUILDING AN ECOSYSTEM FOR CRITICAL MARITIME INFRASTRUCTURE PROTECTION 7
1.3.1. FEASIBILITY STUDY AND STRATEGIC RATIONALE 7
1.3.2. ANCHORING THROUGH RHID AND ECOSYSTEM GOVERNANCE 8
1.3.3. COLLABORATION WITH THE NAVY AND OPERATIONAL STAKEHOLDERS 8
1.3.4. OPPORTUNITY WITHIN THE BLUE BASTION CALL 8
1.4. SUPPORT OF THE BLUE CLUSTER 9
1.5. BLUE BASTION PROJECT INSTRUMENTS 9
1.5.1. BLUE BASTION RESEARCH (TRL 3–5) 10
1.5.2. BLUE BASTION DEMONSTRATOR (TRL 5–6) 11
1.5.3. BLUE BASTION OPERATIONAL INNOVATION (TRL 6–7) 11
1.5.4. INTEGRATED INNOVATION PIPELINE 12
2. BLUE BASTION RESEARCH CALL 13
2.1. OBJECTIVES OF THE BLUE BASTION PROGRAMME 13
2.2. RESEARCH AND ECOSYSTEM BUILDING 14
2.2.1. CORE EXPECTATIONS FOR THE FINAL DELIVERABLE 14
2.2.2. RESEARCH DISSEMINATION AND VALIDATION 15
2.2.3. ACTIVE PARTICIPATION IN THE BLUE CLUSTER ECOSYSTEM 15
2.3. ELIGIBILITY CRITERIA FOR PROJECT PARTNERS 16
2.3.1. NOTES FOR COMPANIES, A(I)SBL AND FOUNDATIONS: 16
2.4. INFORMATION DAY 17
3. CALL INFORMATION 18
3.1. DOCUMENTATION RELATED TO THIS CALL 18
3.2. INDICATIVE CALENDAR OF THE CALL 18
3.3. RESEARCH THEMES AND INDICATIVE BUDGET OF THIS CALL 19

3.3.1. CONTEXT 19
3.3.2. Research Theme 1: Integrated Detection, Attribution & Response for Underwater Threats 20
3.3.3. Research Theme 2: Next-Generation Protection & Resilience of Critical Maritime Infrastructure 22
3.4. PROJECT DURATION 23
3.5. PROJECT PARTNERSHIP 23
3.5.1. PARTNERSHIP 23
3.5.2. STAKEHOLDERS 23
3.5.3. ROLES AND RESPONSIBILITIES WITHIN THE PROJECT 24
3.5.3.1. ROLE OF THE COORDINATOR 24
3.5.3.2. SUBCONTRACTORS 24
3.6. RESEARCH ETHICS 25
3.7. BUDGET RULES 26
3.8. GENDER 28
4. SUBMISSION PROCEDURE 29
4.1. PRE-PROPOSAL 29
4.2. PROPOSAL 30
5. EVALUATION PROCEDURE AND CRITERIA 32
5.1. CONTEXT AND SETUP 32
5.2. FIRST PHAESE: PRE-PROPOSAL 32
5.2.1. STEP 0: PRE-PROPOSAL CONSULTATION 32
5.2.2. STEP 1: ELIGIBILITY CHECK 33
5.2.3. STEP 2: ALIGNMENT CHECK WITH ROADMAP AND SCOPE 33
5.2.4. STEP 3: EVALUATION BY THE SCIENTIFIC ADVISORY BOARD, CHALLENGE OWNERS AND INDUSTRIAL PARTNERS STEERING COMMITTEE 33
5.2.5. STEP 4: CONSOLIDATION AND RECOMMENDATION BY THE BLUE CLUSTER STEERING COMMITTEE 34
5.2.6. STEP 5: FINAL DECISION PRE-PROPOSAL BY RHID AND NAVY 34
5.3. PHASE 2: FULL PROPOSAL 34
5.3.1. Step 1 - Remote scientific peer review evaluation 34
5.3.2. Step 2 - Scientific Experts Committee (SEC) evaluation, including interviews with the applicants 35

5.3.3. Step 3 - Selection proposal formulated by the Scientific Committee of the RHID 36
5.3.4. Step 4 - Final selection of proposals by the Board of Directors of the RHID 37
5.4. EVALUTION CRITERIA 37
6. ROYAL DECREE AND CONTRACTUAL OBLIGATIONS FOR SELECTED PROJECTS.. 38
6.1. PROJECT STARTING AND END DATE 38
6.2. ROYAL DECREE AND CONTRACTS 38
6.3. COMPOSITION AND ROLE OF THE STEERING COMMITTEE 39
6.4. PROJECT MONITORING AND FOLLOW-UP 40
6.5. REPORTS 40
7. DATA, RESULTS, INTELLECTUAL OWNERSHIP AND SECURITY REQUIREMENTS .. 42
7.1. GENERAL CONDITIONS 42
7.2. CLASSIFIED INFORMATION/SECURITY RELATED ACTIVITIES 42
8. COMPLAINTS 45
9. CONTACTS 46

1. RESEARCH, DEVELOPMENT, INNOVATION AND INDUSTRIALIZATION OF THE MINISTRY OF DEFENCE

1.1. CONTEXT

Scientific and technological research in the domain of security and defence is key to maintaining the Belgian Defence military and technological edge, to face current and future security challenges. For this purpose, the Ministry of Defence (2025) (https://www.mil.be/media/ulunodln/strategische-visie-2025-integraal.pdf) seeks to further develop and strengthen the links between Defence, the national research institutions and the industry by gradually increasing its R&T contribution as from 2022, with a view to reaching 2% of the total defence effort in 2030. The setup pf the Blue Cluster ecosystem on the protection of critical maritime infrastructure its perfectly in and contributes to the implementation of this strategic vision and general policy for Defence.

1.2. ROLE OF THE ROYAL HIGHER INSTITUTE FOR DEFENCE - RHID

As a "smart hub" and "honest broker" for scientific and technological research, the Royal Higher Institute for Defence (RHID) is responsible for the development and implementation of the Ministry of Defence's policy on scientific and technological research. Within this policy, twelve focus areas have been identified, in which research is actively supported and stimulated. As a "smart hub", RHID aims to promote the growth of Belgian scientific and technological research in the field of defence and security, as well as to restore and strengthen the links between administrations, universities and companies at this prospect. It wishes to achieve this, among others, by promoting and facilitating the participation of Belgium and the Belgian Ministry of Defence in international, national and regional research programmes. In addition, the results of research are published annually for a wide audience and colloquia are held regularly. As an "honest broker", RHID manages and facilitates, through the department Research, Development, Innovation and Industrialization (RDII), the research programme of the Ministry of Defence. Although in the past this programme was primarily reserved for Defence research institutions, collaboration with other partners, including Belgian research institutes and industry, is increasingly becoming the norm. The Ministry of Defence wants to further develop its capabilities through collaborative research with external partners by launching open calls for proposals within the frame of its research programme. The current call is the first Blue Bastion call as part of development of an ecosystem on maritime security and defence where applicants can propose research and developments projects in the relevant technology domain.

More information on the institute and its activities can be found on the website: https://www.defence institute.be/en/accueil-english/

1.3. BUILDING AN ECOSYSTEM FOR CRITICAL MARITIME INFRASTRUCTURE PROTECTION

The development of an ecosystem for the protection of critical maritime infrastructure originates from the assignment of RHID to the Blue Cluster (www.bluecluster.be) to explore the feasibility and added value of a coordinated, ecosystem-based approach. This assignment reflects the growing strategic importance of maritime domains and the need to move beyond isolated innovation projects towards a structured, scalable, and demand-driven ecosystem that brings together defence, civilian, and dual-use capabilities.

Under this RHID assignment, the Blue Cluster was tasked with assessing how an ecosystem could be built to address emerging threats to ports, offshore energy installations, subsea infrastructure, coastal zones, and maritime traffic. As a neutral innovation orchestrator with strong ties to industry, research organisations, and public authorities, the Blue Cluster is uniquely positioned to align strategic needs with industrial and technological capabilities.

BLUE CLUSTER	The **Blue Cluster** is the industry-driven innovation cluster that brings together companies, knowledge institutions, and public actors active in the blue economy. It stimulates collaboration and innovation across maritime and offshore domains—such as shipping, ports, offshore energy, maritime security, and digital maritime technologies—by connecting stakeholders, facilitating joint projects, and aligning innovation with societal and strategic needs. Acting as a neutral ecosystem orchestrator, the Blue Cluster supports both civilian and dual-use innovation with the aim of strengthening economic resilience and sustainable growth in the maritime domain. https://www.bluecluster.be/

1.3.1. FEASIBILITY STUDY AND STRATEGIC RATIONALE

A dedicated feasibility study, conducted within the framework of the RHID assignment, confirmed both the operational relevance and industrial potential of establishing a maritime security ecosystem. The study highlighted increasing vulnerability of maritime critical infrastructure, the fragmentation of existing solutions, and the need for

integrated approaches combining sensing, surveillance, autonomy, data fusion, and decision support.

The study also demonstrated strong dual-use potential, with overlapping requirements between civilian infrastructure protection and defence-oriented maritime security. It concluded that a coordinated ecosystem—supported by shared testing environments, aligned roadmaps, and sustained stakeholder engagement—would significantly increase innovation efficiency, accelerate deployment, and strengthen resilience at regional and national levels.

See An ecosystem for the protection of critical maritime infrastructure | Blue Cluster

1.3.2. ANCHORING THROUGH RHID AND ECOSYSTEM GOVERNANCE

The RHID assignment provides a structural backbone for transforming the feasibility insights into a concrete innovation pathway. Within this framework, Blue Cluster acts as ecosystem integrator, ensuring coherence between research, industrial development, and operational needs. It lowers entry barriers for SMEs and technology providers, fosters cross-sector collaboration, and connects innovation activities to longer-term defence and security priorities.

This approach shifts the focus from individual technology development to system-level solutions, interoperability, and lifecycle thinking—key elements for effective critical maritime infrastructure protections.

1.3.3. COLLABORATION WITH THE NAVY AND OPERATIONAL STAKEHOLDERS

A cornerstone of the ecosystem is the close collaboration with the Navy, infrastructure owners and maritime security authorities, who are involved early and continuously in the innovation process. Their engagement ensures that solutions are operationally relevant, validated in realistic maritime environments, and aligned with existing operational concepts and standards.

This collaboration also strengthens the bridge between civilian and military domains, reinforcing the dual-use character of the ecosystem and facilitating smoother uptake from pilot demonstration to operational deployment. Blue Cluster plays a central role in structuring this interaction and creating trusted spaces for co-development.

1.3.4. OPPORTUNITY WITHIN THE BLUE BASTION CALL

Within this broader ecosystem context, the Blue Bastion call represents a concrete implementation step. One of its core objectives is to initiate and structure collaborative innovation projects that directly contribute to the protection of critical maritime infrastructure. Rather than funding stand-alone technology developments, the call is designed to stimulate consortium-based projects, bringing together industry,

knowledge institutions, and operational stakeholders around shared maritime security challenges.

To enable this, the action—explicitly named Blue Bastion—provides not only project funding, but also the necessary instruments to support ecosystem formation. This includes mechanisms to lower collaboration barriers, align partners around validated operational needs, and facilitate progression from early-stage concepts towards testing and demonstration. In this sense, project funding acts as a strategic tool to catalyse cooperation, de-risk innovation, and accelerate learning across the ecosystem.

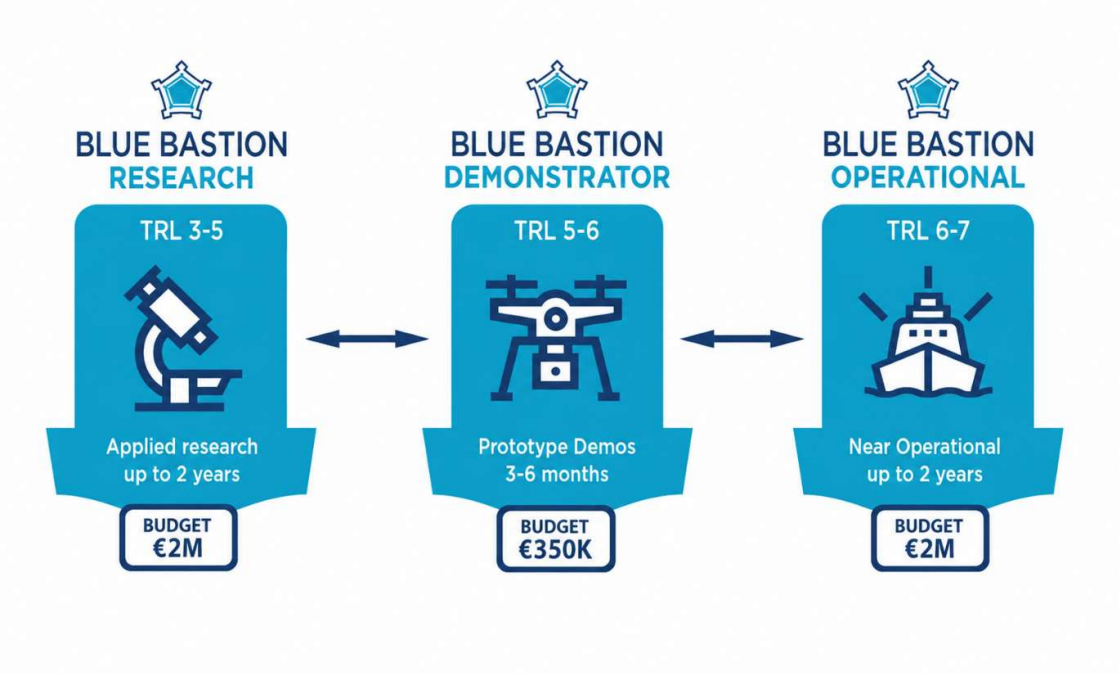
Blue Bastion thus functions as more than a traditional call for proposals. It is an enabling action that strengthens the ecosystem by fostering structured partnerships, encouraging interoperability between solutions, and ensuring that individual projects contribute to a coherent, long-term approach to maritime critical infrastructure protection. Through this action, Blue Cluster reinforces its role as ecosystem orchestrator, translating strategic ambitions and RHID-anchored insights into tangible, collaborative innovation outcomes.

1.4. SUPPORT OF THE BLUE CLUSTER

The Blue Cluster supports Blue Bastion projects throughout their full lifecycle by acting as an ecosystem orchestrator: before the project, it aligns ideas with the maritime security roadmap, mobilises and connects partners, and supports consortium building and proposal shaping; during the project, it facilitates coordination, stakeholder engagement, cross-project synergies and high-visibility demonstrations such as the Navy Captains of Industry Day; and after the project, it ensures valorisation and upscaling of results by promoting outcomes, supporting market and operational uptake, and feeding lessons learned back into the maritime security research and innovation agenda to strengthen the long-term ecosystem for critical maritime infrastructure protection.

1.5. BLUE BASTION PROJECT INSTRUMENTS

The Blue Bastion calls are designed to activate collaborative innovation projects that strengthen the protection of critical maritime infrastructure. This call explicitly focuses on **Blue Bastion Demonstrator** projects, enabling rapid demonstration of potential solutions in relevant maritime environments. In parallel, Blue Bastion also comprises Research and Operational Innovation instruments, which follow a longer-term project logic and are opened on a different schedule.



All projects funded under Blue Bastion must align with the strategic roadmap on maritime security, which provides thematic focus areas, capability priorities, and development pathways for the ecosystem.

Together, these instruments form a coherent portfolio that supports innovation from applied research to near-operational deployment, while ensuring continuity and ecosystem impact. The instruments planned for Blue Bastion include:

1.5.1. BLUE BASTION RESEARCH (TRL 3–5)

Blue Bastion Research targets applied research and early-stage development activities aimed at maturing new concepts, technologies, and methodologies for maritime protection. Projects at this level focus on technical feasibility, functional validation, and concept integration beyond basic research.

Projects must demonstrate clear alignment with the roadmap defined in the feasibility study, ensuring that research efforts contribute to identified ecosystem needs and create progression pathways towards later demonstrator or operational innovation projects.

- Typical activities include proof-of-concept development, laboratory testing, early prototyping, and system modelling.
- Project duration: up to 2 years, with a maximum grant amount of EUR 2 million per project.
- This instrument will be open for applications on a yearly basis, aligned with the standard Blue Cluster project application flow.

1.5.2. BLUE BASTION DEMONSTRATOR (TRL 5–6)

Blue Bastion Demonstrator projects focus on the demonstration of solutions in relevant and representative maritime environments, demonstrating possible integration, performance, and added value under near-realistic conditions. Strong emphasis is placed on collaborative consortia, bringing together industry, knowledge institutions, and where relevant, operational stakeholders.

The focus of demonstrator projects is still on innovation and research (TRL <6) and not on implementation or integration (TRL>6). Demonstrators are the last step in a research and innovation track before starting the implementation and integration track.

Demonstrator projects must be positioned within the feasibility study roadmap, clearly indicating which capability gaps, use cases, or development lines they address and how results will contribute to the broader ecosystem.

- Demonstrator projects are designed as short, focused innovation and research actions, enabling fast learning cycles, risk reduction, and visible progress within the ecosystem.
- Project duration: 3 to 6 months, with a maximum grant amount of EUR 350k per project.

This demonstrator call will be opened twice a year, creating regular opportunities for new consortia to enter the ecosystem and build on previous results.

1.5.3. BLUE BASTION OPERATIONAL INNOVATION (TRL 6–7)

Blue Bastion Operational Innovation supports projects that bring solutions close to operational deployment. Activities may include large-scale testing, pilot implementations, integration with existing systems, and validation with end users in operational contexts.

Projects under this instrument must align with the roadmap from the feasibility study, demonstrating contributions to prioritized operational capabilities and long-term ecosystem objectives.

- The focus is on robustness, interoperability, scalability, and readiness for sustained use in maritime protection operations.
- Project duration: up to 2 years (with a maximum grant amount of EUR 2-5 million per project).
- This instrument will be open on a yearly basis, following the regular Blue Cluster project submission cycle.

1.5.4. INTEGRATED INNOVATION PIPELINE

The three Blue Bastion instruments collectively form an integrated innovation pipeline, anchored in the maritime security roadmap. Short-cycle demonstrator projects deliver rapid validation and momentum, while research and operational innovation projects provide depth, continuity, and long-term impact.

Through this structured approach, Blue Bastion uses project funding as a strategic tool to build collaboration, ensure roadmap coherence, and accelerate ecosystem-wide innovation for maritime critical infrastructure protection.

2. BLUE BASTION RESEARCH CALL

2.1. OBJECTIVES OF THE BLUE BASTION PROGRAMME

- **Advancing research excellence for critical maritime infrastructure protection**: Supporting high-quality applied research (TRL 3–5) addressing strategic maritime security and defence challenges through the development, validation and maturation of innovative technologies and concepts.
- **Building strategic knowledge and future capabilities:** Developing the scientific and technological foundations needed to address emerging threats to critical maritime infrastructure, while contributing to future maritime security and defence capabilities.
- **Building critical mass in maritime security research and innovation:** Creating a strong Belgian knowledge, industrial and technology base around priority maritime security challenges, reinforcing national capabilities, strategic autonomy and future participation in European defence and security value chains.
- **Stimulating collaborative research through consortia:** Bringing together industry, research organisations, knowledge institutions and operational stakeholders to address complex maritime security challenges through multidisciplinary approaches.
- **Developing and validating innovative concepts and technologies:** Advancing promising solutions beyond fundamental research through modelling, proof-of-concept development, laboratory validation, prototype development and experimental testing.
- **Aligning research with the Blue Bastion Maritime Security Roadmap:** Ensuring research activities contribute to priority capability domains and long-term development needs identified by the maritime security ecosystem.
- **Reducing technological uncertainty and increasing maturity:** Generating the evidence, technical validation and scientific understanding required to de-risk emerging technologies before large-scale demonstration and operational deployment.
- **Strengthening the maritime security research ecosystem:** Creating critical mass and reinforcing Belgium's research and innovation capacity in maritime security, defence and critical infrastructure protection.
- **Creating pathways towards European programmes and value chains:** Positioning Belgian actors for participation in future European Defence Fund (EDF), Horizon Europe, NATO DIANA and other international security and defence initiatives.

- **Generating knowledge, intellectual property and future innovation opportunities:** Delivering new scientific insights, methodologies, technologies and exploitable results that can form the basis for future demonstrator and operational innovation projects.
- **Enabling progression towards operational validation and deployment:** Preparing technologies and concepts for transition towards TRL 5–6 demonstrators, operational innovation activities and potential future implementation within maritime security and defence contexts.

2.2. RESEARCH AND ECOSYSTEM BUILDING

The end product of a Blue Bastion Research project is a validated technology, concept, system architecture or prototype for the protection of critical maritime infrastructure, demonstrated in a controlled and representative environment (TRL 3–5). The project must generate new scientific and technological knowledge while providing a clear pathway towards demonstrator projects, operational validation and future deployment in maritime security and defence contexts.

2.2.1. CORE EXPECTATIONS FOR THE FINAL DELIVERABLE

A Blue Bastion Research project is expected to deliver at least:

- Generate new scientific and technological knowledge addressing priority maritime security and critical infrastructure protection challenges.
- Develop and validate an innovative technology, concept, methodology, architecture or prototype beyond the current state of the art.
- Demonstrate feasibility and performance through experimental validation in controlled and representative environments relevant to maritime security applications.
- Contribute to the priority capability domains and research themes identified in the Blue Bastion Maritime Security Roadmap.
- Provide a clear transition pathway towards TRL 5–6 demonstrator projects, including identified use cases, remaining risks and recommendations for further maturation.
- Create value for the broader maritime security ecosystem by strengthening knowledge, industrial capabilities and future innovation opportunities at regional, national and European level.
- Position the developed solutions for future participation in European and international programmes, value chains and collaborative security initiatives.

In essence, a Blue Bastion Research project must deliver validated knowledge and technology that forms the foundation for future demonstrators, operational innovation and deployment in maritime security and defence contexts.

2.2.2. RESEARCH DISSEMINATION AND VALIDATION

The programme requires research results to be actively validated and disseminated to relevant stakeholders:

- At least one research validation event with relevant challenge owners and end users is mandatory. This event should assess the applicability, maturity and potential operational relevance of the developed concepts, technologies or prototypes.
- Projects are expected to demonstrate and discuss key research outcomes with relevant stakeholders, including developed methodologies, prototypes, system concepts, experimental results and identified implementation pathways.
- Where feasible, developed concepts or prototypes should be validated in representative maritime environments or test facilities, supporting the transition from research towards future demonstration and operational innovation activities.
- Projects are encouraged to disseminate non-confidential results through scientific publications, technical papers, conferences, workshops or other relevant communication channels, strengthening knowledge sharing and visibility within the maritime security community.
- Final project results should include recommendations for further maturation and application, identifying opportunities for follow-on demonstrator projects, operational validation and participation in European or international research and innovation programmes.

The objective is to ensure that research outcomes are not limited to scientific knowledge creation but are validated with relevant stakeholders and positioned for future uptake, demonstration and implementation.

2.2.3. ACTIVE PARTICIPATION IN THE BLUE CLUSTER ECOSYSTEM

Active participation in the Blue Cluster ecosystem is a mandatory requirement within a Blue Bastion Research project. This includes, but is not limited to:

- Participation in relevant ecosystem activities (events, workshops, community sessions).
- Knowledge sharing and coordination with other Blue Bastion projects to enhance coherence and complementarity.
- Contributions to the further refinement of the ecosystem roadmap and to the input for the research and innovation agenda.

To enable this active and long-term engagement, all members of a Blue Bastion Research consortium are **members and partners of the Blue Cluster**. The Blue Cluster organisation will actively support consortium partners in this process and

facilitate their integration into the ecosystem, ensuring access to the relevant networks, events, and collaboration opportunities.

Research projects are therefore assessed not only on their technical output, but also on their engagement, collaboration, and contribution to the broader ecosystem.

2.3. ELIGIBILITY CRITERIA FOR PROJECT PARTNERS

This call is open to Belgian public and private non-profit research institutes and private companies.

From the public research sector, all Belgian universities, colleges of higher education, federal scientific institutions, defence research institutes and other public research institutes are eligible partners.

Private non-profit research centres must have operational and/or research activities in Belgium. They must have legal personality and their registered office in Belgium.

From the private sector, companies (including SMEs) complying with the following criteria are eligible partners:

- The company must have operational and/or research activities on the Belgian territory.
- The company must have a legal personality and its registered office in Belgium. The legal personality is required at the latest when signing the research contract.
- At the moment of signing the contract, the company must have fulfilled its obligations to pay its taxes and social security contributions.

All consortium partners (private and non-private) must be members of the Blue Cluster.

Foreign partners cannot participate in the call.

The project partnership is a triple helix composition where academia and industry work together to foster R&T(D) for Defence. Specific partnership requirements are set out in section 3.6.

2.3.1. NOTES FOR COMPANIES, A(I)SBL AND FOUNDATIONS:

The delivery of the following documents is a formal requirement for a valid application for the call:

- As foreseen in the law of 18 September 2017, companies, a(i)sbl and foundations (partners+subcontractors) must have submitted accurate and current information on their beneficial owners to the UBO (Ultimate Beneficial Owner) register of the FPS Finances. The extract of the UBO register must be

provided by e-mail to blue-bastion@blauwecluster.be before 1 October 2026 (23h59).

- The consent form relating to the law of 20 December 2024 on classification and security clearances, security advice and the publicly regulated service (available in Dutch and French on the Blue Bastion website) must be provided for the **coordinator and promotor of each partner and subcontractors**. A negative opinion from the administrative authority for at least one of the persons listed on the UBO may result in the legal entity being refused participation in the project. To be provided by e-mail to IRSD-SECURITY@mil.be before 1 October 2026 (23h59)
- A company Honourability & Vulnerability self-assessment declaration must be delivered to guarantee the company honourability, ethics & professional conduct. This declaration with the related criminal records must be sent by e-mail to blue-bastion@blauwecluster.be before 1 October 2026 (23h59).

Only private companies (including subcontractors) are required to submit the UBO declaration, company honourability declaration, and consent form. Recognised research organisations are not required to submit these documents.

For funded partners and subcontracts: You are a company, a(i)sbl or a foundation?		
Document	**Name and format of the file**	**How to deliver?**
Extract from the UBO-register	ACRONYM_UBO_COMPANY.pdf	E-mail to blue-bastion@blauwecluster.be
Consent form(s) for security verification (coördinator and promotor partners)	ACRONYM_CONSENT_COMPANY_PERSON.pdf	E-mail to IRSD-SECURITY@mil.be
Company Honourability & vulnerability self-assessment declaration + criminal records	ACRONYM_DECLARATION.pdf	E-mail to blue-bastion@blauwecluster.be
Failing to deliver these documents will result in exclusion of the proposal		

2.4. INFORMATION DAY

To inform potential applicants about the context, scope and modalities of this call and to offer them network opportunities, an information day will be held on Wednesday 26 August 2026 in Oostende. Registration prior to the event is required. More details are announced through Blue Bastion website as well as through social media.

3. CALL INFORMATION

3.1. DOCUMENTATION RELATED TO THIS CALL

The following documents are available on the Blue Bastion website (https://www.bluecluster.be/blue-bastion)

- Information:
  - Innovation Roadmap Critical Maritime Infrastructure Protection.
  - Information document, including submission and evaluation guidelines and budget rules: general information on the programme and the call, overview proposal content and corresponding evaluation criteria for the applicants and the evaluators (the present document)
  - Blue Cluster membership overview and application
  - Annex II: General conditions applicable to the 2025 contracts.
- Proposal templates
  - Project-idea 2 pager.
  - Pre-Proposal structure (word-file available on the website platform)
  - Proposal structure (word-file available on the website platform)
  - Template Data Management Plan
  - Template Veiligheidsverificatie toestemming – Vérification de sécurité consentement
  - Template Company Honourability & Vulnerability self-assessment declaration
  - Template Ethics self-assessment
  - Template Gantt chart
  - Template Budget file

3.2. INDICATIVE CALENDAR OF THE CALL

	Date	**At/via**
Ideation phase	June-August	Blue Cluster
Information session	26 Augusts 2026	Oostende
Deadline pre-proposal	1 October 2026 (23h59)	Mail
Eligibility and alignment check	8 October 2026	Blue Cluster & RHID
Steering Comite evaluation	28 October 2026	Blue Cluster
Final selection of pre-proposals	30 October 2026	RHID
Communication of results to applicants	30 October 2026	Mail
Deadline proposal	1 December 2026	Mail
External evaluation	8 January 2027	Blue Cluster
Panel evaluation	1 February 2027	RHID
Final decision proposal	15 February 2027	RHID
Communication of results to applicants	16 February 2027	Blue Cluster

Start research projects	1 April 2027	Consortia

3.3. RESEARCH THEMES AND INDICATIVE BUDGET OF THIS CALL

The present call covers the theme of Critical Maritime Infrastructure Protection as defined by the maritime security roadmap with 2 specific subthemes.

The maximum subsidy budget per project is up to 2,000,000 EUR. Applicants should take into consideration the most efficient use of public resources.

The final number of funded projects may vary depending on the evaluation results and available budget. Passing the threshold of excellence and quality, the best ranked proposals will be funded. The proposals will be put together in a ranking list based on their final evaluation.

Budget transfers between the projects are possible.

3.3.1. CONTEXT

The North Sea and Belgian ports have become strategic hubs for energy supply, digital infrastructure and international logistics, while at the same time becoming increasingly vulnerable to hybrid threats such as sabotage, cyberattacks, underwater intrusions and conventional military actions.

Belgium possesses strong knowledge and industrial capabilities in domains such as mine countermeasures, autonomous underwater systems, sensor integration and AI-driven data fusion, with recognised excellence within EU and NATO frameworks. The innovation roadmap applies the **DDIRR model (Deter, Detect & Identify, Respond, Repair)** as a guiding framework to address maritime security and defence in an integrated and future-oriented manner, with a clear focus on dual-use technologies and public-private cooperation.

The roadmap identifies a coherent set of priorities that together form the maritime security ecosystem:

- **Surveillance and sensor networks (fixed and mobile):** Multimodal detection above, on and below the water surface using radar, cameras, sonar and smart buoys, supported by AI and sensor fusion for persistent situational awareness.
- **Drones and autonomous platforms (UAV, USV, UUV):** Autonomous systems capable of coordinated operations (swarming) for ISR, mine countermeasures, perimeter protection and response, with emphasis on robustness in GPS-denied environments.
- **Automation and robotics:** Infrastructure-bound and mobile systems that partially automate detection, response and recovery, including underwater robotics for inspection, neutralisation and repair.

- **Communication and connectivity:** Secure, redundant and interoperable networks (satellite communications, offshore 5G, acoustic underwater communications) that are resilient to jamming and spoofing and enable seamless data exchange.
- **Data analytics and artificial intelligence:** AI-based threat detection, predictive analysis, multisource data integration and decision support, while keeping humans in the loop.
- **Cybersecurity and digital resilience:** Secure-by-design architectures, real-time cyber-threat detection, redundancy and recovery capabilities for maritime operational and IT systems.
- Collaboration and interoperability: Civil-military and international cooperation, shared standards and test environments to accelerate the transition of innovation to operational use.

For defence, the roadmap delivers targeted reinforcement of maritime operational capability and resilience:

- Enhanced deterrence and protection of critical maritime and subsea infrastructure (Underwater Domain Protection).
- Faster and more accurate detection and identification of threats through integrated ISR chains and AI-enabled situational awareness.
- Flexible and scalable response options through autonomous systems and manned-unmanned teaming, including in hybrid threat scenarios.
- Improved resilience and recovery capacity after physical or cyber incidents through robotic repair and cyber resilience.
- International interoperability and alignment with EU and NATO missions, positioning Belgium as a frontrunner in autonomous and underwater technologies.

In summary, the innovation roadmap provides a clear strategic framework to directly link technological innovation in the Blue Bastion projects to operational defence needs, using dual-use innovation as a lever for both security and industrial strengthening.

3.3.2. Research Theme 1: Integrated Detection, Attribution & Response for Underwater Threats

Context:

Subsea cables, offshore energy infrastructure, ports, shipping routes and naval assets are increasingly exposed to underwater risks. Detecting small, slow-moving, passive or difficult-to-observe objects remains challenging, particularly in congested waters with poor visibility and complex acoustic conditions. Maritime Security Challenge Oweners

have therefore identified integrated underwater detection, threat interpretation and timely intervention as shared priorities.

At the same time, underwater threats rarely occur in isolation and may be linked to activities, assets or threat actors operating across the maritime, land and air domains. Effective protection therefore requires a multi-domain situational awareness approach and seamless communication and information exchange between defence, maritime authorities, infrastructure operators, emergency services and other relevant stakeholders.

Research scope:

Research should develop and experimentally validate an integrated approach for detecting, classifying, attributing and responding to underwater threats. This may include (each project should at least tackle two topics):

- detection of small, passive, biologically masked or low-signature objects;
- underwater imaging in turbid and congested waters;
- differentiation between normal activity, anomalies, sabotage and hostile preparation;
- legal, technical and operational conditions for intervention;
- preventive and proportionate response concepts.
- integration of underwater observations with relevant air, surface and land-based surveillance systems to enable multi-domain threat assessment and attribution;
- secure and interoperable communication mechanisms supporting information sharing, coordination and decision-making between defence, maritime security authorities, critical infrastructure operators and other operational stakeholders.

The research should deliver an integrated system architecture and functional prototype, validated in at least two representative environments, such as an offshore energy site and a port or nautical access zone. The architecture should demonstrate how underwater threat information can be fused with cross-domain data sources and communicated effectively to relevant stakeholders to support coordinated operational responses.

Impact for defence and maritime security

The theme supports the transition from fragmented sensor observations to reliable underwater threat detection, attribution and response. It will strengthen the protection

of naval assets, ports, offshore energy infrastructure and subsea connections, while enabling faster and better-informed intervention by defence, maritime security and infrastructure operators.

By fostering multi-domain situational awareness and improved stakeholder coordination, the research will contribute to a more coherent and resilient security posture across maritime, land and air domains.

3.3.3. Research Theme 2: Next-Generation Protection & Resilience of Critical Maritime Infrastructure

Context:

Critical maritime infrastructure is increasingly exposed to physical, autonomous and hybrid threats targeting offshore energy assets, subsea cables, ports, locks and nautical infrastructure. Detection alone is insufficient: infrastructure must become harder to disrupt, better able to maintain critical functions and faster to recover following an incident. This reflects stakeholder priorities concerning physical protection, security-by-design, energy resilience and operational continuity. Given the increasingly interconnected nature of security threats, solutions should also consider relevant interfaces with land- and air-domain surveillance and protection capabilities.

Research Scope

Research should develop and experimentally validate new technologies and design concepts that strengthen the physical protection and resilience of maritime infrastructure. This may include (each project should al least tackle two topics):

- adaptive barriers and protected zones around critical assets;
- security-by-design for ports, offshore assets, cables and nautical infrastructure;
- autonomous inspection, local protection and intervention systems;
- damage assessment and robotic support for repair;
- temporary energy, communication or operational continuity solutions;
- rapid recovery and reconfiguration of critical infrastructure.
- integration with relevant land- and air-domain monitoring and security systems to support a coherent 360° protection approach

Projects should go beyond desk research by delivering at least one functional prototype, scale model or experimental subsystem, tested in a controlled facility and a representative maritime environment.

Impact for defence and maritime security

The theme will make critical maritime infrastructure intrinsically more resistant to sabotage, autonomous threats and cascading disruption. It will improve the capacity of defence organisations, ports, maritime authorities and energy operators to protect strategic assets, sustain essential functions and restore operations rapidly following an incident.

3.4. PROJECT DURATION

The projects will have a duration of maximum 24 months.

3.5. PROJECT PARTNERSHIP

3.5.1. PARTNERSHIP

Partnerships between research and industry are **mandatory**. Each project consortium must include at least:

- one private company; and
- one research organisation.

Any type of participating organisation may act as project coordinator.

No single project partner may claim more than **80% of the total subsidy awarded to the demo project**.

Belgian Defence research institutes (Royal Military Academy (RMA), Military Hospital Queen Astrid (MHQA), the Defence Laboratories (DLD)) and Blue Cluster are eligible partners. However, it will not have a beneficial effect on the evaluation result (no bonus).

An organisation can only submit one project as coordinator per call.

3.5.2. STAKEHOLDERS

Blue Bastion Research projects are expected to engage their stakeholders—such as end users, infrastructure operators, authorities, and industry partners—in a structured and continuous way throughout the project, by involving them early in defining use cases and requirements, actively seeking feedback during development and testing, and validating results in real or realistic operational settings. The Blue Cluster will support the consortium in this task.

This close interaction ensures that Research projects address concrete operational needs, are technically and organisationally feasible, and gain early support from potential adopters. Effective stakeholder engagement is therefore critical to maximise the relevance, credibility, and impact of the research track, to accelerate learning for all parties involved, and to increase the likelihood that project outcomes can be successfully scaled, adopted, or transitioned into follow-on research, innovation, or operational deployment.

3.5.3. ROLES AND RESPONSIBILITIES WITHIN THE PROJECT

Project partners jointly share obligations and responsibilities during the implementation of the project. The project should be fairly balanced, even if different partners may have different tasks and subsequently different budgets.

A coordinator must be appointed in each network proposal.

For each project, a Steering Committee shall be established at the start of the project to act as the governing body (see section 6.3).

3.5.3.1. ROLE OF THE COORDINATOR

The coordinator is responsible for the overall project management and coordination. He/she is the contact person for the RHID to communicate with the partnership and must transfer all relevant information to the other project partners. He/she shall:

- Coordinate all activities to be carried out in the framework of the project,
- Coordinate the internal meetings between the network members,
- Coordinate the production of the required project reports intended for Belgian Defence as described in section 6.4.,
- Coordinate the synthesis and translation of the research results, with a view to applications and support for decision-making,
- Coordinate the publication and dissemination of the research results,
- Convene meetings of the Steering Committee and write the reports of these meetings. The coordinator shall give notice in writing of a meeting with the agenda to each member no later than fourteen (14) calendar days in advance,
- Inform the Steering Committee and the RHID of any problems that might hinder the implementation of the project.

3.5.3.2. SUBCONTRACTORS

The project may require specific or punctual expertise, which can be delivered in the form of subcontracting. It is the responsibility of the project team to ensure that the

rules and practices of the subcontractor, and in particular the ownership and valorisation of research results, publications and communications, are compatible with the rules governing the call. The project team takes full responsibility for the final result of the subcontracted work.

Subcontractors must be registered in Belgium. Subcontractors that are companies, a(i)sbl and foundations must submit accurate and current information on their beneficial owners to the UBO (Ultimate Beneficial Owner) register of the FPS Finances and deliver an extract of the UBO register to the DEFRA secretariat.

In case the subcontractor needs access to classified information, the subcontractor must also obtain a security clearance (see section 7.2).

- Subcontractors must be registered in Belgium. If they are a company, a(i)sbl or foundation, they must provide:
- An extract from the UBO register (to blue-bastion@blauwecluster.be)
- Security verification consent (form) (to IRSD-SECURITY@mil.be)
- Company honourability & vulnerability awareness self-assessment + criminal records (to blue-bastion@blauwecluster.be)

3.6. RESEARCH ETHICS

The "Code of Ethics for Scientific Research in Belgium" is a joint initiative of the Académie Royale des Sciences, des Lettres et des Beaux-Arts de Belgique, the Académie Royale de Médecine de Belgique, the Koninklijke Vlaamse Academie van België voor Wetenschappen en Kunsten and the Koninklijke Academie voor Geneeskunde van België.

All projects must take this code of ethics into account in their research. If applicable, it is the responsibility of the applicants to consult the relevant Ethical Board for their organisation before submitting a proposal.

The code of ethics for scientific research in Belgium is available here http://www.belspo.be/belspo/organisation/publ/pub_ostc/Eth_code/ethcode_en.pdf

It is the responsibility of the applicants to consult the relevant Ethical Board for their organisation before submitting a proposal.

Applicants will be required to complete an “ethics self-assessment” when preparing the proposal. The Ethical Advisory Board of the RHID will assess this information and can advise the partnership how to deal with the ethical aspects of its proposal.

3.7. BUDGET RULES

Financing by Defence: The selected projects are entitled to receive state aid following approach:

- Financing by Defence: This call is subject to the European legislation on State Funding (Art 107 (1) TFEU and the General Block Exemption Regulation in particular.

Therefore, financing a public research institute or a private non-profit research centre is set to a maximum of 100% of the eligible costs. Financing a private company is limited to a maximum of 65% of the eligible costs (large enterprise), with a potential maximum of 80% (small enterprise & medium enterprise), according to the size of the company.

Small, Medium-sized and Large enterprises are defined as in the Commission Recommendation of 6 May 2003 concerning the definition of micro, small and medium-sized enterprises (Text with EEA relevance) (notified under document number C(2003) 1422)[1]

The total project budget must be detailed in the tables of the budget file (100% cost) of the full proposal. Additional columns are foreseen to indicate the partner contribution to the total project cost (depending on the partner type) and the subsequent RHID funding contribution. (section 6.5 of the full proposal template: Budget assessment)

The project budget is reserved exclusively for the project activities. The different categories of expenditure financed by Defence are:

Staff: Pre-tax wages associated with increases in the cost of living, employers' social security and statutory insurance contributions, as well as any other compensation or allowance due by law and secondary to the salary itself. Defence does not allow cumulative wages for staff. Staff members bound contractually to a public institution - full time or part time - cannot apply for him/herself for Defence staff budget for that part.

The RHID prefers staff to be hired under a labour contract.

Costs related to non-employee staff, i.e. staff working in a management company, as freelancer or interim staff on behalf of the partner are also accepted.

Tax-free doctoral or post-doctoral scholarships are not accepted.

[1] 2EUR-Lex - 02013R1407-20231025 - EN - EUR-Lex 3EUR-Lex - 52022XC1028(03) - EN - EUR-Lex 4"Following application of the protection of Belgian Essential Security Interests invoking Art 346, 1,b of the TFEU" 5EUR-Lex - 32003H0361 - EN - EUR-Lex

For persons to be hired for the project (so not identified by name in the proposal), the staff costs are limited to a maximum amount of:

- 5 700 €/month FTE for a technician/bachelor (regardless of years of experience)
- 8 000 €/month FTE for a Master (regardless of years of experience)
- 8 700 €/month FTE for a Master in engineering (regardless of years of experience)
- 10 500 €/month FTE for a PhD (regardless of years of experience)

The funding is limited to the time and period in which the (employee and non-employee) staff participates in the project.

General operating costs: This category covers minor, recurrent operating expenses that are directly related to the implementation of the project but are not linked to a specific project task, deliverable or dedicated project activity. This includes, for example, usual supplies and consumables for laboratories, workshops and offices, documentation and consignments, standard use of existing software and IT facilities, and the organisation of internal project meetings. The general operating budget may not exceed 15% of the overall project staff budget for the project coordinator and 10% for the other project partners. The amounts claimed must correspond to actual expenditures incurred and strictly related to the project, even where supporting documents are not required to be submitted as part of the regular project reporting. No detailed justification of each individual general operating cost is required in the proposal or during reporting. However, the administration of the concerned partner must retain the relevant invoices and accounting records so that the expenditures can be verified in the event of an audit.

Costs that are directly linked to a specific project task, deliverable or dedicated activity and that can be individually identified and substantiated must be reported under Specific operating costs instead. Costs covered by the overhead allowance may not be claimed as general operating costs. The same underlying expenditure may only be claimed under one cost category.

Specific operating costs: this includes a list of operating costs specific to the execution of the project tasks, such as costs for project analyses, testing, maintenance and repair of equipment purchased by the project, use of specific IT facilities and software, costs for surveys, open data publications, organisation of workshops and events, etc. These costs need to be clearly described in the proposal and each of them shall be justified by invoices during the project.

Overheads: Institutions' general overheads that cover, in one lump sum, administration, telephone, postal, maintenance, heating, lighting, electricity, rent, machine depreciation, and insurance costs. The total amount of this item is set as a fix amount of 10% of the total staff and operating costs.

Equipment: List of investment goods specific to the implementation of the project and to be purchased on the project budget. It concerns the purchase and installation of scientific and technical equipment and instruments, Blue Bastion - Call for proposals 2026 including computer equipment, to be entered in the inventory or assets of the institute/company. Equipment needs to be clearly described in the proposal and shall be justified by invoices.

Investments: General or structural investments are **not eligible project costs**. This includes expenditure primarily intended to create, expand or upgrade long-term operational capacity, infrastructure or fixed assets of the organisation rather than to implement the specific project. Examples include buildings, construction works, major infrastructure, permanent installations, production facilities, general-purpose machinery or equipment intended mainly for commercial or operational use beyond the project. The determining criterion (equipment vs investments) is whether the equipment is specifically required and justified for the implementation of the Blue Bastion project, rather than constituting a broader investment in the organisation's infrastructure or operational capacity.

Subcontracting: Expenses incurred by a third party to carry out project tasks or provide services that require special scientific or technical competences outside the partner's normal area of activity. The amount may not exceed 25% of the total budget allocated to the partner concerned. If the subcontractor is not yet known then only the nature, the planned duration and the estimated amount needs to be indicated in the proposal.

	STAFF COSTS (monthly costs)	GENERAL OPERATION COSTS	SPECIFIC OPERATION COSTS	OVERHEADS	EQUIPMENT	SUBCONTRACTING
PROJECT COORDINATOR	**Technician**: 5 700€/month	15% of Staff costs *(Automatically generated)*	-	10% of [Staff costs + Operation costs] *(Automatically generated)*	-	Max. 25% of the total budget of this partner
	Master: 8 000€/month					
	Master (engineering): 8 700€/month					
	PhD: 10 500€/month					
OTHER PROJECT PARTNERS	**Technician**: 5 700€/month	10% of Staff costs *(Automatically generated)*	-	10% of [Staff costs + Operation costs] *(Automatically generated)*	-	Max. 25% of the total budget of this partner
	Master: 8 000€/month					
	Master (engineering): 8 700€/month					
	PhD: 10 500€/month					

3.8. GENDER

The RHID strongly encourages the applicants to take into account the equality between women and men and to ensure gender mainstreaming in the implementation of the project. The project should include this both in the choice of the researchers and, where relevant, by integrating the gender dimension into their research.

4. SUBMISSION PROCEDURE

The submission of projects will be done in two phases using the following structure:

4.1. PRE-PROPOSAL

Your pre-proposal and the required documents must be submitted at the latest on 1 October 2026 (23h59) by e-mail to blue-bastion@blauwecluster.be

The pre-proposal templates can be downloaded from the website and must contain all following information:

Project pre-proposal (document should be limited to 10 pages + 1 page title/metadata)

- The title and acronym of the project
- Keywords
- Theme
- Coordinates of the foreseen partners (funded and non-funded)
- PROPOSAL
    - Executive Summary of the project (0,5 p)
    - Graphical overview project concept (0,5 p)
    - Scope and objectives (1 p)
    - State of the art and innovative character (1p)
    - Relevance and potential impact (1p)
    - Quality of the project consortium (1p)
    - Methodology (1p)
    - Work plan: work packages (3p)
    - Risk assessment (1p)

As a separate document which can be downloaded from the website:

- The GANTT chart
- Data Management Plan
- Budget file
- Ethics Self-Assessment

Companies, a(i)sbl and foundations (partners and subcontractors) must deliver the extract of the **Ultimate Beneficial Owner (UBO)** register as an annex to the proposal (in pdf format) and sent it by e-mail to blue-bastion@blauwecluster.be . The same applies

to the document **"Company Honourability & Vulnerability self-assessment declaration" and the related criminal records.**

The form "veiligheidsverificatie_toestemming / vérification de sécurité_consentement" of **the coordinator and promotors of the industrial partners** must be sent to IRSD-SECURITY@mil.be .

Please provide these documents grouped by proposal. RHID and Blue Cluster will perform an eligibility and alignment check based on the proposal documents. The proposals that have passed the eligibility and alignment check will be evaluated, see next section

4.2. PROPOSAL

Consortia that have passed the first round are invited to submit their proposal and the required documents at the latest on 1 December 2026 (23h59) by e-mail to blue-bastion@blauwecluster.be

Consortia will be invited to submit a full proposal. The project objectives of the full proposal may vary from that of the pre-proposal to some extent. However, it cannot diverge to the point that the expertise mobilised for the evaluation of the proposal will become irrelevant.

Changes in the project partnership (changes in participating institute(s)/company(ies), including the coordination role) can only be accepted after the explicit approval of RHID (question via Blue Cluster). The keywords must remain the same since they are used for composing the evaluation panel. In case other companies, a(i)sbl and foundations join the network, they must provide the extract of the Ultimate Beneficial Owner (UBO) + other necessary documents register to the call secretariat by e-mail to blue-bastion@blauwecluster.be .

The proposal templates can be downloaded from the website and must contain all following information (the proposal is an elaboration of the pre-proposal with more detail, same template also for the separate documents):

Project proposal (document should be limited to 30 pages + 1 page title/metadata)

- The title and acronym of the project
- Keywords
- Theme
- Coordinates of the foreseen partners (funded and non-funded)

- PROPOSAL
    - Executive Summary of the project (1 p)
    - Graphical overview project concept (1 p)
    - Scope and objectives (2 p)
    - State of the art and innovative character (2p)
    - Relevance and potential impact (2p)
    - Quality of the project consortium (4p)
    - Methodology (4p)
    - Work plan: work packages (10p)
    - Risk assessment (4p)

As a separate document which can be downloaded from the website:

- The GANTT chart
- Data Management Plan
- Budget file
- Ethics Self-Assessment
- Cash or in-kind commitment letter (not-mandatory)

5. EVALUATION PROCEDURE AND CRITERIA

Only proposals that are complete and submitted on time will be taken into account.

5.1. CONTEXT AND SETUP

The Blue Bastion Research programme combines a challenge-driven pre-selection process with a scientific peer-review evaluation procedure to ensure that funded projects are both scientifically excellent and strategically relevant for maritime security and critical maritime infrastructure protection.

The selection process consists of two consecutive phases:

- **Phase 1 – Pre-Proposal:** A strategic screening process coordinated by The Blue Cluster, RHID and the Navy to assess eligibility, alignment with the Blue Bastion scope and roadmap, operational relevance, implementation feasibility and expected impact.
- **Phase 2 – Full Proposal:** An in-depth scientific evaluation process, based on independent peer review, expert panel assessment and scientific committee review, ensuring scientific excellence and alignment with Defence priorities.

Together, these phases ensure that selected projects combine scientific excellence, technological innovation, operational relevance, industrial potential and strategic value for maritime security and critical infrastructure protection.

5.2. FIRST PHAESE: PRE-PROPOSAL

5.2.1. STEP 0: PRE-PROPOSAL CONSULTATION

Prior to the submission of a full proposal, applicants are strongly encouraged to discuss their project idea with The Blue Cluster innovation managers by means of a concise two-page pre-proposal (see template). This pre-proposal outlines the project concept, visual overview, intended objectives, envisaged consortium, addressed use cases, and its preliminary alignment with the Blue Bastion scope and roadmap. Blue Cluster aligns with RHID and Navy on the status and progress of the pre-proposal phase.

The purpose of this step is to:

- provide early feedback on strategic fit with the Blue Bastion programme,
- identify potential improvements in scope, focus, or consortium composition,
- and facilitate early connection with relevant ecosystem partners where appropriate.

Deadline pre-proposal consultation: 18 September 2026

This consultation is non-binding and does not constitute a formal evaluation, but it aims to increase the quality and relevance of full proposals submitted to the call.

5.2.2. STEP 1: ELIGIBILITY CHECK

Blue Cluster and RHID will perform an eligibility check on the basis of the proposal documents. Following criteria are applied:

- Completeness of the proposal
  - All fields fully completed
  - UBO extracts available
  - Company Honourability & Vulnerability self-assessment declaration
  - Additional documents available)(see section 4.1)
- Invitation to submit the the form “veiligheidsverificatie_toestemming / vérification de sécurité_consentement”
- Eligibility of each project partner (see section 2.3),
- Partnership composition (see section 3.6.1).
- Membership of Blue Cluster.

5.2.3. STEP 2: ALIGNMENT CHECK WITH ROADMAP AND SCOPE

As a second step, RHID, The Blue Cluster, and the Navy jointly assess the proposal’s alignment with the Blue Bastion roadmap and the scope of the call. This assessment verifies that the proposal:

- falls clearly within the thematic and strategic focus of the call,
- contributes to the capability priorities identified in the roadmap,

The outcome of this step is a documented alignment check, which forms the basis for the subsequent in-depth evaluation.

5.2.4. STEP 3: EVALUATION BY THE SCIENTIFIC ADVISORY BOARD, CHALLENGE OWNERS AND INDUSTRIAL PARTNERS STEERING COMMITTEE

Eligible and aligned proposals are subsequently evaluated by three different boards focussing on three different criteria providing a score and feedback.

- **Excellence (Scientific Advisory Board):** Assessment of the quality, level of innovation, state of the art, TRL, methodology, and validation approach.
- **Implementation (Industrial Partners Steering Committee):** Assessment of the feasibility of the work plan, timing, budget, quality of the consortium, task distribution, integration, and risks.

- **Impact (Challenge Owners):** Assessment of the expected impact/added value, adoption, scalability, valorisation, and contribution to future use or capability development.

The individual scores and feedback are consolidated into one score and feedback for each criterium/group.

5.2.5. STEP 4: CONSOLIDATION AND RECOMMENDATION BY THE BLUE CLUSTER STEERING COMMITTEE

Building on the evaluation results of STEP 3, the Blue Cluster Maritime Security Steering Committee of industrial partners performs an integrated assessment of the proposal.

The Steering Committee considers strategic coherence, overall portfolio balance, feasibility, industrial possibilities and expected economic impact. Based on this assessment, the Steering Committee prepares a substantiated evaluation proposal, including a recommendation (e.g. recommended, recommended under conditions, or not recommended), which is submitted to RHID.

5.2.6. STEP 5: FINAL DECISION PRE-PROPOSAL BY RHID AND NAVY

RHID makes the final funding decision, taking into consideration the evaluation proposal prepared by the Steering Committee and the strategic objectives of the programme.

5.3. PHASE 2: FULL PROPOSAL

The selection of full proposals is based on a peer-review evaluation that guarantees scientific excellence and the alignment of the projects with the thematic objectives of the call. The evaluation of the full proposals runs in four steps:

- Step 1 - Remote scientific peer review evaluation
- Step 2 - Scientific Experts Committee (SEC) evaluation, including interviews with the applicants
- Step 3 - Selection proposal formulated by the Scientific Committee of the RHID
- Step 4 - Final selection of proposals by the Board of Directors of the RHID

5.3.1. Step 1 - Remote scientific peer review evaluation

The BLUE CLUSTER organises and coordinates a scientific peer review evaluation of each proposal. The principles of this evaluation are the same for all themes.

Each of the full proposals will be evaluated by a team of independent experts having an adequate combined expertise to evaluate the research proposal. Ideally, each expert team will be composed of minimum one Belgian and minimum one foreign expert.

For each proposal, an individual written evaluation is performed. The written evaluation takes place remotely based on an evaluation form. During this assessment, the experts will only have access to the proposals they will evaluate. They will not know who the other two reviewers are for that proposal, nor will they have access to each other's evaluations.

Each reviewer will assess the proposal and provide comments taking into account the evaluation criteria and also provides a score.

The applicants will receive a compilation of the remote evaluators' feedback (anonymised). They will also get the list of questions to which they must answer in writing before the interview. This list might include questions from the Ethical Advisory Board of the RHID.

5.3.2. Step 2 - Scientific Experts Committee (SEC) evaluation, including interviews with the applicants

According to the scores obtained of the external evaluators, the proposals will be ranked in a list (proposal ranking). This list will serve as a base for the panel discussion.

Scientific Experts Committee (SEC) evaluation

For each theme, the Scientific Expert Committee of Defence will be composed of members that are relevant for the theme. Each SEC will have access to the full proposals (and annexes), the anonymised evaluation reports and the proposal ranking of the theme + the scores and feedback of the BLUE BASTION steering committee for the pre-proposals.

Each SEC will organise interviews with the applicants of the full proposals according to the following schedule:

- Introduction (5 minutes)
- Presentation by the applicants, including an introduction of the proposal and integrating the answers to the questions of the remote experts and Ethical Advisory Board (15 minutes).
- Questions and answers (Q&A) (25 minutes).
- Deliberation (10 minutes).

The applicants will assist in the meeting for the presentation and Q&A session of their proposal only.

Each SEC will classify the full proposals into (a) Panel Funding Scenario(s) according to BLUE BASTION evaluation criteria:

The SEC Funding Scenario(s) will classify all proposals in:

- Recommended for funding.

- Not recommended for funding.

The SEC will list the proposals that are recommended for funding by order of their final evaluation result.

5.3.3. Step 3 - Selection proposal formulated by the Scientific Committee of the RHID

After the Scientific Experts Committee meetings, the best ranked proposal(s) per theme will be proposed for funding to the Scientific Committee of the RHID. The remaining proposals will be put together in a common ranking list based on their final evaluation results.

The Scientific Committee of the RHID is composed of senior scientists and research directors and guarantees the quality level of Defence research. It proposes evaluation methods and research objectives, participates in the drafting of the research programme (ranking and selection of research projects) and evaluates its implementation. The composition of the Scientific Committee is currently defined in the Ministerial Decree of 11 January 2022.

The Scientific Committee will receive the following documents:

- SEC Funding Scenarios(s) per theme, including its motivation
- Common ranking list of all proposals across all themes, earmarking the best ranked proposal for each theme
- Full proposal and evaluation reports of each proposal (on demand)
- Feedback and score of the pre-proposal by the Blue Cluster steering committee.

Based on these documents, the Scientific Committee will perform a strategic selection of the proposals based on the criteria and rules explained hereunder, delivering the Scientific Committee Funding Scenario.

The following aspects will be taken into account when formulating the Scientific Committee Funding Scenario to the governance board of the RHID:

- Alignment of the proposal in relation to Defence priorities
- Added value of the proposal in relation to Defence priorities

The Scientific Committee will formulate the Scientific Committee Funding Scenario taking into account the

- In NO case will proposals deemed ‘out of scope’ be considered
- In NO case will proposals deemed ‘not recommended for funding’ be considered

5.3.4. Step 4 - Final selection of proposals by the Board of Directors of the RHID

The final selection decision of proposals to be funded is made by the Board of Directors of the RHID on the basis of the Scientific Committee Funding Scenario.

5.4. EVALUTION CRITERIA

The scientific board, challenge owners and industrial partners, Steering Committee, external evaluators, panel and RHID all assess and score proposals against the following three criteria:

- **Excellence:** The quality of the proposal, based on the clarity of the project objectives, the level of innovation with respect to the state of the art, the targeted TRL, the methodology, and the proposed validation approach.
- **Implementation:** The quality and adequacy of the partnership and the feasibility of the implementation, taking into account the work plan, timing, budget, task distribution, integration between partners and activities, and the management of key risks.
- **Impact:** The relevance and potential impact for Defence, including the expected added value, potential for adoption and scalability, valorisation prospects, and contribution to future operational use or capability development.

Each criterion is scored on a scale from **0 to 5**. A minimum score of **3/5** must be achieved for each criterion. Proposals receiving a score between **3 and 4** on a criterion may be subject to **additional conditions or recommendations**, which must be addressed during project implementation or prior to the project start.

These complementary evaluations ensure that selected Blue Bastion Research projects are strategically aligned, scientifically sound, operationally relevant, and capable of delivering tangible impact for Defence and other relevant challenge owners in the field of protection critical maritime protection.

The individual evaluations are not communicated to the applicants.

6. ROYAL DECREE AND CONTRACTUAL OBLIGATIONS FOR SELECTED PROJECTS

6.1. PROJECT STARTING AND END DATE

The projects selected within the context of the current call will start 1 April 2027.

The project contracts will have a duration of 24 months plus 1 month to allow meeting all administrative requirements before the effective start-up of the project).

6.2. ROYAL DECREE AND CONTRACTS

For the selected proposals, a Royal Decree is decided, and a contract is conducted between Belgian Defence and the funded partners.

The contract is composed of three parts that make up the research contract:

- Basic Contract
- Annex I: Technical specifications
- Annex II: General conditions applicable to the 2026 contracts.

The basic contract designates the contracting parties (partners and Defence) and contains the general obligations applicable to the project, including the project and contract duration and budget. The basic contract is signed by the heads of the partners involved (directors, rectors, CEOs).

The content of Annex I “Technical specifications” is specifically related to the operational implementation of the project. It includes the detailed work description and schedule, details on funding by expenditure category etc.

Annex I “Technical specifications” is signed by the Blue Bastion programme manager and the promotors concerned.

Annex II “General conditions applicable to the contract” contains all general provisions applicable to all Blue Bastion contracts. It will be made available on the Blue Bastion website and will not be signed.

Belgian Defence/RHID grants the selected projects the funds required for their implementation. The RHID shall reimburse at most, and up to the amount specified in the granted budget, the actual costs proven by the partners providing these costs are directly related to the implementation of the project.

The partnership is encouraged to conclude a Consortium Agreement to define internal regulations regarding intellectual property (access to foreground and background, valorisation rights and modalities, and any other theme deemed necessary). A copy of the signed Consortium Agreement must be handed over to the Royal Higher Institute for Defence (RHID and blue-bastion@blauwecluster.be).

6.3. COMPOSITION AND ROLE OF THE STEERING COMMITTEE

Each project will be accompanied by a Steering Committee, to be set up at the start of the project. The Steering Committee is composed of the project managers of the partners, the programme manager, the research manager of Defence and the intended end user.

The Steering Committee acts as a governance body, to ensure that the project remains in line with the research objectives and adapt the project plan accordingly whenever necessary. It ensures that the project reporting is done in accordance with section 6.4.

The Steering Committee should meet at least once a month to discuss the project's progress.

The organisation of such meeting must be included in the project work plan and the project budget.

The following actions and decisions will be taken by the Steering Committee:

- Examine information collected by the coordinator on the progress of the Project, to assess the compliance of the Project with the Proposal and, if necessary, propose modification of the Proposal.
- Determine the policy for press releases, joint publications and other public disclosures regarding the Project.
- Keep a register of Foreground generated within the Project and patents filed thereon, which is concluded at the end of the Project.
- Examine and approve proposed changes to the work programme. In case of actions with a budgetary impact, the Steering Committee will make proposals to the funding authority but cannot decide without the approval of this funding authority.
- If necessary, propose the termination of all or part of the Project.

6.4. PROJECT MONITORING AND FOLLOW-UP

For each selected project, a dedicated Blue Cluster **(DBC) Innovation Manager** will be assigned as the main point of contact for project monitoring, coordination, and follow-up.

The following monitoring and follow-up structure is foreseen for all projects:

- **Kick-off meeting** organised at the start of the project, with participation from all project partners, DBC, RHID/KHID, the Belgian Navy and, where relevant, other key stakeholders. The meeting will confirm the project scope, planning, responsibilities, expected results and reporting arrangements.
- **Quarterly coordination meetings** held between the DBC Innovation Manager and the project coordinator to review progress, upcoming activities, risks, issues and any required corrective actions.
- **Mid-term review** organised approximately three months after project start, involving the same key stakeholders as the kick-off meeting. The review will assess progress against the objectives, milestones, budget and expected demonstration results.
- **Final review and demonstration** organised at the end of the 2-year project period. The project partners will present the achieved results and demonstrate the developed solution/research output or capability to the relevant stakeholders.

Project partners are expected to actively participate in this follow-up process and to timely communicate any significant deviations, delays, risks or changes that may affect the successful implementation of the project.

6.5. REPORTS

The contract foresees the following reports to be submitted to Blue Cluster and RHID:

- **Initial report:** to be submitted within three weeks of the start of the project.
- **Progress report(s):** to be submitted according to the specifications in the contract (annex 1, technical specifications).
- **Final report:** to be submitted one month after the end of the project.

- If deemed useful by the RHID, an additional report may be requested for an external evaluation of the project.
- The RHID can ask for a report or other input at any time during the course of the project in order to provide scientific support to valorisation and service actions related to the programme.

These reports are to be included in the project work plan and the cost of preparing them (including possible translations) must be covered by the project budget. They should contain all necessary information to assess the progress of the project in relation to the work packages, deliverables and budget. Problems must be identified, including possible solutions.

To evaluate the impact of the Blue Bastion programme, the RHID can ask input from the partnership until 3 years after the end of the project.

7. DATA, RESULTS, INTELLECTUAL OWNERSHIP AND SECURITY REQUIREMENTS

7.1. GENERAL CONDITIONS

The Data Management Plan (DMP), to be submitted as part of the proposal, describes how the project partners deal with the collected data before, during and after the project. It is a key element of good data management.

For all aspects regarding the use of data, intellectual ownership and valorisation of the project results and the confidentiality or security requirements, the conditions of the General Conditions (Annex II of the contract and the articles 12, 13 and 14 in particular) apply.

Ownership of existing information and data (the individual background) remains with the original owner.

As a principle, the Foreground - the results (including information) produced by the project - shall be the property of the partner carrying out the work generating this foreground.

The principles for the use of joint foreground will have to be determined by the project partners, with respect for these General Conditions. These principles can be included in a Consortium Agreement to be concluded between the partners.

7.2. CLASSIFIED INFORMATION/SECURITY RELATED ACTIVITIES

Projects aiming at developing or using sensitive or classified information's will not be funded by Blue Bastion. However, certain activities undertaken in the frame of the projects may generate classified information. This paragraph solely concerns protective measures to be taken to preserve the confidentiality of security-sensitive information regarding these projects.

A classification is given to documents to prevent their improper use which could damage, among other things, the fulfilment of the tasks of Defence, the external security and international relations of the State and the scientific and economic potential of the country (for the complete list see "Wet van 20 Dec 2024 Art 3/Loi du 20 Déc 2024 Art 3").

According to the same law this identification should be based on the following classification levels:

- The "TRES SECRET/ZEER GEHEIM" level is assigned to a piece if its improper use could cause EXTREMELY SERIOUS damage to the main Belgian interests listed in the law. Topics that qualify under this category cannot be part of the project. •

- The "SECRET/GEHEIM" level is assigned to a document if its improper use could cause SERIOUSLY damage to the interests listed in the law.
- The "CONFIDENTIEL/VERTROUWELIJK" level is assigned to a document if its improper use could harm any of the interests listed in the law.

Documents of which the originator wants to limit the distribution to persons who are authorized to use them on a need-to-know basis, without however attaching legal consequences to this limitation, are marked with the indication "DIFFUSION RESTREINTE/BEPERKTE VERSPREIDING".

These classification levels should be applied both to the need to protect information and the need to avoid unnecessary obstruction to the use of research information and results.

Applicants should identify in the proposal the classification needs for the work packages of the project that involve threat and /or vulnerability assessments and the information on specifications or capabilities of the tool(s) used.

- threat assessments (i.e. estimation of the likelihood of a malicious act against an asset, with particular reference to factors such as intention, capacity and potential impact)
- vulnerability assessments (i.e. description of gaps or weaknesses which can be exploited during malicious acts, and often contain suggestions to eliminate or diminish these weaknesses)
- specifications (i.e. exact guidelines on the design, composition, manufacture, maintenance or operation of threat substances or countermeasure substances, technologies and procedures)
- capability assessments (i.e. description of the ability of an asset, system, network, service or authority to fulfil its intended role — and in particular the capacity of units, installations, systems, technologies, substances and personnel that have security-related functions to carry these out successfully.

Based on the assessment of the provided input a security screening by Belgian Defence might be imposed in the contract on ALL partners and subcontractors of the selected project(s). In that case, these beneficiaries should obtain a security clearance before starting work on classified parts of the project.

The applicable security framework for the action must be in place at the latest before the signature of the contract and will be considered as an annex to the contract. More information can be found on the website of the National Security Authority (Nationale Veiligheidsoverheid – Autorité Nationale de Sécurité) https://www.nvoans.be/

Persons that are involved in a project must be nationals of a country of the European Union or nationals of a country of the European Free Trade Association or nationals of a

country that is a member of NATO. Persons involved in a project may be subject to a verification. Only after a positive verification, a person can be recruited to the project.

8. COMPLAINTS

RHID and Blue Cluster places great importance on the quality of their service and on improving the way they operate. RHID and Blue Cluster will handle complaints about the administrative handling of this call for proposals and/or about content of the call and the contracts that are concluded as a result of the call.

A special form to handle complaints has been created. The complaint form is available through the website of Blue Bastion.

Complaints submitted anonymously or which are offensive or not related to our organisation will not be processed.

A complaint is handled as follows:

- Once your complaint has been filed, a notification of receipt will be sent.
- The complaint will be forwarded to the relevant departments and individuals and will be processed within one month.
- An answer will be sent by e-mail or letter.
- The complaint will be treated with strict confidentiality.

If you are dissatisfied by the initial response to a complaint, you can always contact the Médiateur Fédéral / Federal Ombudsman, rue de Louvain 48 bte 6 / Leuvenseweg 48 bus 6, 1000 Brussels (email: contact@mediateurfederal.be / contact@federaalombudsman.be).

9. CONTACTS

Further information can be obtained by contacting: blue-bastion@blauwecluster.be