

**DEFRA** Defence-related Research Action

# Call for proposals 2024 Information document including submission and evaluation guidelines and budget rules

# **Important dates:**

Information day: 25 January 2024 (8h30 - 16h30) Deadline Pre-proposals: 22 February 2024 (14h00) Deadline Full proposals: 18 April 2024 (14h00)

For more information on the programme, please visit <u>https://www.belspo.be/defra</u>





# TABLE OF CONTENTS

| ТА |                  | CONTENTS  |    |
|----|------------------|---|----|
| 1. | SCIE             | NTIFIC AND TECHNOLOGICAL RESEARCH OF THE MINISTRY OF DEFENCE                    | 3  |
|    | 1.1.             | CONTEXT   |    |
|    | 1.2.             | ROLE OF THE ROYAL HIGHER INSTITUTE FOR DEFENCE - RHID                           | .3 |
|    | 1.3.             | COLLABORATION WITH THE FEDERAL SCIENCE POLICY – BELSPO                          |    |
| 2. | DEFE             | NCE-RELATED RESEARCH ACTION – DEFRA   | 4  |
|    | 2.1.             | OBJECTIVES OF THE PROGRAMME   | .4 |
|    | 2.2.             | ELIGIBILITY CRITERIA FOR PROJECT PARTNERS                                       | .4 |
|    | 2.3.             | INFORMATION DAY   | .5 |
| 3. | CALL             | INFORMATION   | 5  |
|    | 3.1.             | DOCUMENTATION RELATED TO THIS CALL  | .5 |
|    | 3.1.1.           |   | -  |
|    | 3.1.2.           |   |    |
|    | 3.2.             | INDICATIVE CALENDAR OF THE CALL   |    |
|    | 3.3.             | RESEARCH THEMES AND INDICATIVE BUDGET OF THIS CALL                              |    |
|    | 3.3.1.           |   |    |
|    | 3.3.2.           |   |    |
|    | 3.3.3.           |   |    |
|    |                  | DATA SYSTEMS TO RENDER DATA INTO ACTIONABLE DATA                                | -  |
|    | 3.3.4.           | THEME 4 – NEXT-GENERATION VISION AND SENSOR FUSION                              |    |
|    | 3.3.5.           |   |    |
|    | 3.3.6.           |   |    |
|    | 3.4.             | PROJECT DURATION  |    |
|    | 3.5.             | PROJECT PARTNERSHIP   |    |
|    | 3.5.1.<br>3.5.2. |   |    |
|    | 5.5.2.           | ROLE OF THE COORDINATOR   |    |
|    |                  | SUBCONTRACTORS  |    |
|    | 3.6.             | RESEARCH ETHICS   | -  |
|    | 3.7.             | BUDGET RULES  | -  |
|    | 3.8.             | GENDER  |    |
| 4  |                  | AISSION PROCEDURE   | -  |
|    | 4.1.             | PHASE 1 – PRE-PROPOSAL  |    |
|    | 4.2.             | PHASE 2 – FULL PROPOSAL   | -  |
| 5. |                  | UATION PROCEDURE AND CRITERIA   |    |
|    | 5.1.             | EVALUATION PROCEDURE  |    |
|    | 5.1.1.           | PHASE 1 – EVALUATION OF PRE-PROPOSALS   |    |
|    | 5.1.2.           |   |    |
|    |                  | STEP 1 - REMOTE SCIENTIFIC PEER REVIEW EVALUATION                               | 21 |
|    |                  | STEP 2 – SCIENTIFIC EXPERTS COMMITTEE EVALUATION, INCLUDING INTERVIEWS WITH THE |    |
|    |                  | APPLICANTS  | 22 |
|    |                  | STEP 3 - SELECTION PROPOSAL FORMULATED BY THE SCIENTIFIC COMMITTEE OF THE RHID  | 23 |
|    |                  | STEP 4 - FINAL SELECTION OF PROPOSALS BY THE BOARD of DIRECTORS OF THE RHID     | 24 |
|    | 5.2.             | EVALUATION CRITERIA   | 24 |
| 6. | CONT             | RACTUAL OBLIGATIONS FOR SELECTED PROJECTS                                       | 24 |
|    | 6.1.             | PROJECT STARTING AND END DATE   | 24 |
|    | 6.2.             | CONTRACTS   |    |
|    | 6.3.             | COMPOSITION AND ROLE OF THE STEERING COMMITTEE                                  | 25 |
|    | 6.4.             | REPORTS   |    |
| 7. | DATA             | A, RESULTS, INTELLECTUAL OWNERSHIP AND SECURITY REQUIREMENTS                    | 26 |
|    | 7.1.             | GENERAL CONDITIONS  | -  |
|    | 7.2.             | SPECIFIC CONDITIONS   |    |
|    | 7.3.             | CLASSIFIED INFORMATION/SECURITY RELATED ACTIVITIES                              |    |
|    |                  | PLAINTS   |    |
| 9. | CONT             | TACTS   | 28 |

# **1. SCIENTIFIC AND TECHNOLOGICAL RESEARCH 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 (2023)<sup>1</sup> 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 of the Defence-related Research Action - DEFRA - fits 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 Scientific and Technological Research of Defence (STRD), 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 annual open calls for proposals within the frame of its research programme. The current call is the fourth DEFRA call, based on five (5) well-defined research themes and one (1) open call in which applicants can propose research on Innovative and Future-Oriented Defence Solutions.

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

#### 1.3. COLLABORATION WITH THE FEDERAL SCIENCE POLICY – BELSPO

For organising and managing the DEFRA calls for proposals, a long-term collaboration agreement has been signed on 13 December 2021 between the Ministry of Defence and the Federal Science Policy (BELSPO). BELSPO will

<sup>&</sup>lt;sup>1</sup> Policy Declaration Defence 2023

manage these calls for proposals on behalf of the Ministry of Defence. For the selected projects, funding is granted by and contracts will be concluded with the Ministry of Defence.

# 2. DEFENCE-RELATED RESEARCH ACTION – DEFRA

#### 2.1. OBJECTIVES OF THE PROGRAMME

Through the funding of research projects based on scientific excellence, the DEFRA programme allows meeting the scientific knowledge needs of the Belgian Defence.

The general objectives of the programme are the following:

- Support and strengthen scientific excellence.
- Develop and realise a critical research mass on themes considered to be a priority for Belgian Defence in order to:
  - contribute to short- and long-term capacity development, in line with the Integrated Capability Development Plan (ICDP) and the Strategic Vision for Defence.
  - contribute to the culture of innovation planned within Defence, both in terms of technology and process improvement.
  - foster employment for Defence.
  - contribute, in accordance with the Defence, Industry and Research Strategy (DIRS), to the development of a competitive and credible national industrial and technological base in the field of security and defence.
- Encourage the participation of highly qualified Belgian research institutes and industry in Defence and security related research activities.
- Promote systemic, multidisciplinary/interdisciplinary and integrative approaches.
- Strengthen transdisciplinary research in order to enable potential users to make better use of the research achievements.

#### This is the **fourth call** in the frame of the DEFRA programme.

#### 2.2. ELIGIBILITY CRITERIA FOR PROJECT PARTNERS

This call is open to Belgian public and private non-profit research institutes and private companies (both as funded and non-funded partners in the project).

The project partnership must be in a triple helix composition where academia and industry work together to foster R&T for Defence (see section 0).

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.

Specific partnership requirements per theme are set out in section 3.5.

Research institutes and/or companies external to the project (other than funded and non-funded project partners) can confirm their interest and commitment to provide input to the project via cash or in-kind contributions by completing the cash or in-kind commitment letter available on the platform.

**NOTE:** As foreseen in the law of 18 September 2017, **companies**, **a(i)sbl and foundations** must have submitted accurate and current information on their beneficial owners to the UBO (Ultimate Beneficial Owner) register of the FPS Finances. **The delivery of an extract of the UBO register is a formal requirement for a valid application for the call.** 

You are a company, a(i)sbl or a foundation? Upload your UBO register in the online platform!

The documents of the applicants are submitted to the General Intelligence and Security Service which will examine them in accordance with its missions and legal powers as defined in the law of November 30, 1998 governing intelligence and security services. The advice rendered by the security service may be based on a classified note.

#### 2.3. 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 **Thursday 25 January 2024 (8h30 – 16h30) at the Royal Military Academy.** 

Registration prior to the event is required.

More details are announced through the **DEFRA-website** and the <u>website of the RHID</u> as well as through <u>social</u> <u>media</u>.

# 3. CALL INFORMATION

# 3.1. DOCUMENTATION RELATED TO THIS CALL

#### 3.1.1. DEFRA WEBSITE

The following documents are available on the **DEFRA website** (https://www.belspo.be/defra):

• 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)

- Evaluators eligibility: eligibility criteria for potential remote evaluators
- Evaluation matrix for pre-proposals: overview of the evaluation ratings for the pre-proposals
- Evaluation matrix for full proposals: overview of the evaluation ratings for the full proposals
- Platform Submission guidelines: information for the applicants on the use of the submission platform
- FAQ
- Pre-proposal structure (word-file available on online platform)
- Full Proposal structure (word-file available on online platform)
- Annexe II general conditions applicable to the 2024 contracts

# 3.1.2. DEFRA SUBMISSION PLATFORM

The following templates will be made available on the **DEFRA online SUBMISSION platform** (<u>https://defra.belspo.be</u>) and must be used compulsorily unless otherwise stated. Applicants must log in to the

platform in order to access them:

In PHASE 1 of the call (submission of pre-proposals):

• Pre-proposal template (Word file)

In PHASE 2 of the call the following documents will be made accessible to the applicants that are invited to submit a full proposal:

- Full Proposal template (Word file) only accessible to the selected pre-proposals
- Gantt chart (Excel file)
- Cash or in-kind commitment letter (from institutes/companies which are not partners of the project) non mandatory, only if applicable (Word file)

|   | Date                     | At / via                      |
|---|--------------------------|-------------------------------|
| Information session                         | 25 January 2024 (8h30 –  | RMA, building I, meeting room |
|   | 16h30)                   | Frank De Winne                |
| Deadline Pre-proposals                      | 22 February 2024 (14h00) | Online submission platform    |
| Communication of evaluation result pre-     | 14 March 2024            | Mail                          |
| proposals                                   |                          |                               |
| Deadline Full proposals                     | 18 April 2024 (14h00)    | Online submission platform    |
| Remote scientific peer review evaluation    | 22 April – 31 May 2024   | Online evaluation platform    |
| Feedback to applicants in preparation of    | 21 June 2024             | Mail                          |
| panel meeting (consensus reports and        |                          |                               |
| questions to applicants)                    |                          |                               |
| Written feedback by applicants (answers)    | 26 July 2024             | Mail                          |
| Panel evaluation, incl. interviews with the | Between 22 August and 4  | RHID                          |
| applicants                                  | September 2024           |                               |
| Selection proposal formulated by the        | 12 September 2024        | NA                            |
| scientific committee of the RHID            |                          |                               |
| Final selection of proposals by the board   | 24 September 2024        | NA                            |
| of directors of the RHID and allocation of  |                          |                               |
| projects                                    |                          |                               |
| Communication of results to applicants      | 27 September 2024        | Mail                          |
| Signature contracts                         | 14 November 2024         | Online E-sign platform        |

# 3.2. INDICATIVE CALENDAR OF THE CALL

# 3.3. RESEARCH THEMES AND INDICATIVE BUDGET OF THIS CALL

The present call covers the following research themes, with their indicative budget:

|  | Indicative budget<br>(M€) |
|--|---------------------------|
| Theme 1 – CYBER: Short-term Mitigation Techniques for Software Resilience  | 1,8                       |
| Theme 2 – Securing critical Maritime Infrastructure  | 1,8                       |
| <b>Theme 3</b> - Improved <b>Underwater Communications</b> between Sensors/Weapon Systems and Data systems to Render Data into Actionable Data | 1,8                       |
| Theme 4 – Next-Generation Vision and Sensor Fusion   | 1,8                       |
| Theme 5 – Prolonged Forward Casualty Care  | 1,8                       |
| Theme 6 – Open Call: Research on Innovative and Future-Oriented Defence Solutions  | 3,0                       |
| TOTAL  | 12,0                      |

There is no set maximum budget per project. However, applicants should take into consideration the total available budget for each theme. The objective is to develop a project with the most efficient use of public resources.

The number of projects that will be funded per theme depends on the evaluation of the proposals and the requested budget per proposal. It is envisaged to have 1 or more projects funded for each of the themes. Budget transfers between the themes are possible.

Proposals can only be introduced in the "Open call" if the subject of the proposal does not correspond with one of the other five themes.

# 3.3.1. THEME 1 - CYBER: SHORT-TERM MITIGATION TECHNIQUES FOR SOFTWARE RESILIENCE

#### Context

Most currently used systems are still (partially) written in programming languages that lack memory safety, resulting in countless vulnerabilities that continue to be found in the systems we are using on a daily basis. Migrating these systems to memory safe languages (e.g. Rust) will require a very long conversion time and an abrupt change of the full code base.

Therefore other, more short-term solutions are needed to harden current-day software and cyber-physical systems. A number of conceptual solutions exist, for instance in the form of a wide range of mitigations that can prevent the exploitation of vulnerabilities. Examples include advanced forms of temporal and spatial software diversity that go beyond Address Space Layout Randomization (ASLR), and various instantiations of software integrity policies such as Control Flow Integrity (CFI), Data Flow Integrity (DFI), SafeStack, bounds checking, sandboxing, multi-variant execution, (partial) migration to safe programming languages, etc.

The uptake of these solutions is however hampered because of various shortcomings that have not yet been addressed sufficiently by the research community, such as a sometimes considerable performance impact, being prone to denial-of-service attacks, in certain cases compatibility issues, etc.

There is reason to believe, however, that most of those mitigations can be further developed to become usable, at least in specific security-critical usage scenarios and under some assumptions. The goal is therefore to develop these concepts into technology demonstrators that are validated for specific military use cases.

#### **Research scope**

The software used in the information systems and cyber-physical systems that are found in a military environment, relies to a large extent on legacy code. Due to the inevitable programming faults in this code, in combination with the unsafe programming languages used, these systems suffer from hidden security vulnerabilities that – when discovered by an attacker – could be exploited and possibly lead to remote code execution attacks.

This call is therefore open to research that addresses defensive mechanisms for protecting existing software, written in insecure programming languages, that might contain vulnerable code. A number of such protection mechanisms have already been proposed in the scientific literature. The research shall select existing mechanisms, improve them and/or propose innovative solutions, and demonstrate their feasibility and effectiveness.

The final aim is to improve the security of both existing and newly developed systems by providing developers with a set of tools and best practices that allow them to incorporate protective mechanisms in the development process, while being in control of the tradeoff between the overhead caused by the protection mechanisms and the effort required to bypass them.

The applicants will therefore focus on the following aspects:

- Innovative solutions to harden legacy software written in C and/or C++.
- Performance, DoS resistance of these solutions.
- Compatibility and Comparison with existing approaches.

#### Impact for Defence

The proposals must address technologies and solutions in the area of software protection mechanisms and provision a technology validation at TRL 5 on one or more practical use cases that are relevant for a military environment.

The goal is to facilitate the development of more secure information systems and cyber-physical systems, and as a result contribute to the force protection objective and reduce the number of security incidents.

# 3.3.2. THEME 2 – SECURING CRITICAL MARITIME INFRASTRUCTURE

#### Context

The presence of critical infrastructure, including cables, windmills, artificial islands and pipelines, in Belgian North Sea (TTW-EEZ) and beyond, requires robust measures to ensure their protection. This becomes even more crucial considering future projects like the energy island in the Belgian North Sea, which will hold strategic importance for Belgium's energy infrastructure. It is essential for Belgian Defence to be prepared to contribute to the safeguarding of the maritime infrastructure against non-malicious and malicious threats when, not if, called upon.

# Research scope

In addition to cyber security measures, physical security plays a vital role in protecting critical maritime infrastructure. Implementing physical barriers and access control mechanisms around these assets helps deter unauthorized access and strengthens overall security.

To enhance these measures, robust perimeter monitoring systems and/or maritime unmanned systems can:

- Provide real-time situational awareness to authorities like the "Maritiem Informatiekruispunt" (MIK) or the Maritime Operations Centre (MOC)
- Conduct regular inspections in order to detect anomalies
- Identify potential threats
- Provide non-lethal and lethal capabilities to deter or neutralize identified threats

It is important to recognize the complexity of the involved domains surface, air, cyber and specifically underwater.

The research should have specific attention on the challenges:

- Balance between delayed versus real-time data dissemination
- Maximum effectiveness with minimal collateral damage (in the largest sense: ecological, economical, military,...)
- Trade-off ranging from single use sensor/effector to permanent observation/neutralization
- Maximum probability of detection with minimum probability of false alerts

#### Impact for Defence

This call aims to facilitate the research (for the Belgian Defence) of a credible and realistic architecture for the protection of Belgium's maritime critical infrastructure, taking into account the existing legal framework and all other competent parties involved.

The solution, in accordance with the research scope, could encompass

- either a comprehensive framework, considering the unique challenges of the underwater environment and the multi-domain nature of the protection requirements
- or a combination of sensors, effectors,... that addresses specific challenges.

Ideally, the offered solution should be compatible with the existing and future systems in the "Maritiem Informatiekruispunt" (MIK) and the Maritime Operations Centre (MOC).

# 3.3.3. THEME 3 – IMPROVED **UNDERWATER COMMUNICATIONS** BETWEEN SENSORS/WEAPON SYSTEMS AND DATA SYSTEMS TO RENDER DATA INTO ACTIONABLE DATA

#### Context

Advancements in underwater communication technology have the potential to revolutionize the integration between sensors, weapon systems and data, enhancing situational awareness and targeting data for improved operational effectiveness in the maritime domain. Advancements, namely in wireless networks, robotics, localisation, ranging and tracking, are obvious candidates to look into. However, effectively managing and processing the anticipated abundance of information, particularly from unmanned systems, poses a significant challenge in real-time. The complex underwater environment with its intricate acoustic pathways, limited visibility, changing salinity profiles and corrosive conditions further compounds the difficulties.

### Research scope

Improvements in high-bandwidth acoustic modems (capable of robust and rapid data transmission over required distances), signal processing algorithms, adaptive coding techniques are a few examples, which could enhance data transmission capabilities, optimizing bandwidth utilization.

Additionally, research could develop solutions to enable comprehensive data fusion, resulting in improved maritime situational awareness and targeting capabilities. Research should focus on delivering advancements in automatic detection, classification and identification algorithms, along with the integration of multi-sensor input, including distributed acoustic sensing.

Research projects are expected to focus on:

- Improved (underwater) data transmission on a qualitative and quantitative level (robust and rapid data transmission)
- Enhanced decision-making processes (in the underwater domain): data fusion, data visualisation, data processing,...
- Underwater automatic detection, classification and identification

#### Impact for Defence

In order to accelerate progress in underwater communications/transmission, this call aims to develop a demonstrator that can help to overcome the existing challenges in either the data transmission domain, the (acoustic) data fusion domain or the challenge of localisation, tracking and ranging.

Conducted research should be applied in the naval mine warfare or in another relevant maritime domain.

# 3.3.4. THEME 4 – NEXT-GENERATION VISION AND SENSOR FUSION

#### Context

Advances in detector technology, computing power, digital data and signal processing, have paved the way for better Electro-Optical/InfraRed (EO/IR) systems, with better Detection, Recognition and Identification (DRI) characteristics, and a higher level of automation.

Day and thermal (MWIR/LWIR – Medium Wave IR / Long Wave IR) sensors continue to increase in resolution and framerates, and decrease in size; additionally, a strong progress can be found in the domains of Short Wave IR (SWIR) sensors, multi/hyperspectral filter technologies and low light CMOS sensing. The technological evolutions at sensor level open up many options, but also pose several challenges due to the increased bandwidth, with associated technical challenges, and increased amount of information, with the associated increase in cognitive load.

The level of multi-sensor integration when using different EO/IR systems together often still remains limited. The principle of edge computing can be used to deepen the level of integration and to increase the quality of the obtained information. For that, state-of-the-art embedded hardware and advanced image processing techniques will be needed. On one hand, the DRI for human vision can be improved by post-processing algorithms and visually combining information from different sensors in a user-friendly way. On the other hand, the strong advances in machine learning can be applied to increase the autonomy of the EO/IR system.

#### Research scope

Research efforts should have the goal to, starting from a set of EO/IR sensing capabilities:

- Extract actionable information from a combination of sensors: visible, SWIR, MWIR, LWIR but also multispectral and, possibly, hyperspectral sensors, the two latter being inherently multi-sensor.
- Create enhanced vision capabilities in such a way that the complex and diverse sensor data are intelligently combined to simplify the load of data going to the user, and/or in that way that the sensor system provides processed data to deliver the right information to the user (with the possibility of suggesting a decision to the user).

Examples are the implementation of high reliability automatic detection, identification and track systems or the generation of metadata to be used for assisted decision making by the operator (or at a higher level of the system). Another challenge lies in performing edge computing, i.e. with relatively constrained resources and without manual operator intervention prior to the downlinking of the processed data. Depending on the application, all the processing might have to be performed close to the sensor, or the processing might be split between the platform on which the sensors are mounted and a processing centre where the processed sensor information may be combined with additional information (historical information or data from other modalities such as maps).

In all cases, the reliability of the information should be as high as possible to facilitate the alert of and decisionmaking by the operator. Attention will be paid to the timeliness of the provided information, i.e. the time between the acquisition of the data by the sensor and the delivery of the actionable information to the end-user. This might further constraint the type of processing that can be performed and the processing architecture. The sensor systems' integration and interoperability with other sensors (networks) and connection to battlefield management systems can also be addressed.

#### Impact for Defence

Multi- and hyperspectral imaging is particularly useful in military surveillance and reconnaissance because of countermeasures that adversaries now take to avoid (airborne) surveillance. Pulling information from such a large portion of the spectrum should create unique spectral signatures of equipment, ammunition, and personnel.

This not only improves the ability to counter the latest camouflage developments but also provides more certainty on the identification of decoys.

It is evident that the need for a translation from the hyperspectral image to what an operator understands is necessary, helping the operator, shooter, or commander to take faster and better decisions.

Apart from surveillance, two more fields of specific interest were identified:

1. The stand-off capability to detect IED, UXO and mine indicators.

2. The stand-off capability to detect CBRN-agents. Insertion of current sensors into contaminated areas always implies decontamination afterwards. This impedes on the speed of re-use and pertains certain risks for the operators. A stand-off capability would not only provide a solution to the problems mentioned, but hyperspectral imaging shows the potential to quickly establish knowledge on the extent of the contaminated area, the propagation of CBRN-agents and would help accuracy on predictive modelling.

This action seeks to build a demonstrator for either lightweight electro-optical devices (man-portable or deployed on a Class1 UAS < 150 kg) or for high-end platform mounted systems that can be tailored to specific applications for Belgian Defence.

# 3.3.5. THEME 5 – PROLONGED FAR FORWARD CASUALTY CARE

#### Context

This call aims to support consortia engaged in innovative research and development efforts to enhance the provision of care for wounded soldiers on the battlefield, particularly in situations where immediate medical assistance is not readily available. Recent insights from the conflict in Ukraine learn that immediate evacuation from the frontline is often not possible. This is in contrast with the recent conflicts where NATO nations were involved. Therefore, appropriate solutions must be provided. Scientific research projects could show a new way of dealing with this major issue.

We encourage interdisciplinary collaborations and creative solutions that leverage technology to empower fellow soldiers to provide extended care to the wounded for hours or even days until evacuation becomes possible.

#### **Research scope**

The primary objective of this research initiative is to explore novel approaches, tools, and technologies that enable soldiers, referred to as "buddies," to deliver effective and sustained care to injured comrades in far forward and hostile environments. The proposed research could address one or more of the following areas (not limitative and only listed as an example) that are of particular interest for the Belgian Defence:

<u>Remote Assistance</u>: Develop methods to remotely assess and treat the condition of wounded soldiers using artificial intelligence for medical treatment protocols, enabling medics and buddies to provide timely and appropriate care. This may involve the integration of wearable sensors, telemedicine or other innovative approaches.

<u>Drones for extended care</u>: e.g. Develop pre-programmed "push" drones for medical supply able to bring large amount of equipment to remote areas. The same drones should be able to be used in a "pull" mode to evacuate out of the hostile environment a sick or injured patient while being medically monitored.

<u>Homemade instruments tailored to the treatment:</u> Explore the use of 3D-printing on the field using a preprogrammed printing list of medico-surgical consumables to enhance the capabilities of buddies in treating injuries.

<u>Multi power rewarming system</u>: Design and develop a light and efficient rewarming system for tents or closed environments that can use different kind of energy sources. A cooling patient has less chance of survival than a patient with normal core temperature. Since logistic chains are sometimes broken, the use of local sources of energy provided by the direct environment will help providing the best prolonged casualty care in austere situations.

Interested consortia are invited to submit research proposals that align with the research focus areas outlined above. The proposals should demonstrate a clear understanding of the challenges associated with prolonged far forward casualty care and propose innovative solutions to address them.

#### Impact for Defence

We look forward to receiving innovative and impactful research proposals that have the potential to revolutionize the field of prolonged far forward casualty care. The large scope of potential future, yet unknown, battlefields will force military and civilian first responders to be agile and highly mobile by using disruptive technologies to be able to respond in an efficient and effective way to save lives. The present research call will influence the way the tactical combat casualty care could be provided by using technologies by improving care and evacuations. This will therefore also impact positively the workload and standards of care down the complete medical care chain. Together, we can make a difference in ensuring the welfare and survival of our soldiers on the battlefield.

# 3.3.6. THEME 6 – **OPEN CALL**: RESEARCH ON INNOVATIVE AND FUTURE-ORIENTED DEFENCE SOLUTIONS

#### Context

Proposals are welcome to address new, upcoming, or unforeseen challenges and/or creative or disruptive solutions. Proposals can only be introduced in the "open theme" if the subject of the proposal does not correspond with one of the other 5 themes.

#### **Research scope**

This call is open to any research for defence across a broad spectrum within the following defence research areas:

- Space technologies
- Communication Technologies
- Sensor Technologies
- Autonomous Systems and Artificial Intelligence
- Cybersecurity
- Smart and Advanced Materials
- Advanced Weapon Systems and Platforms
- Protection of Personnel, Systems, and Infrastructure
- Sustainable Energy and Environment
- Advanced Military Health
- Human Systems and Behaviour
- Security and Defence Policy

#### **Impact for Defence**

Proposals should focus on innovative defence technologies and solutions, including within the social and human sciences, that can improve readiness, deployability and sustainability across all spectrums of tasks and missions, for example in operations, equipment, infrastructure, energy solutions and surveillance systems.

The aim of this open call is to realize innovative and cost-effective solutions for defence applications, groundbreaking or novel concepts, new promising future improvements or the application of technologies that have not previously been applied in the defence sector.

#### 3.4. PROJECT DURATION

The projects will have a duration of **2 to maximum 4 years**.

# 3.5. PROJECT PARTNERSHIP

# 3.5.1. PARTNERSHIP

For all themes, proposals must be submitted by a **network** composed of **at least one** (public or private non-profit) **research institute** - receiving at least 10% of the project budget - **and one private company**. All types of organisations can act as project coordinator<sup>2</sup>.

#### Partnership:

- at least one (public or private non-profit) research institute
  - at least one company

Belgian Defence research institutes (Royal Military Academy (RMA), Military Hospital Queen Astrid (MHQA) and the Defence Laboratories (DLD)) can be a partner in the network<sup>3</sup>. Except for theme 1<sup>\*</sup>, it is not mandatory to have one of these institutes as a partner; it will neither have a beneficial effect on the evaluation result (no bonus).

\*For **theme 1 – CYBER**, it is **MANDATORY** to have the Royal Military Academy (RMA) as a partner in the network.

# 3.5.2. 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.).

#### ROLE OF THE COORDINATOR

The coordinator is responsible for the overall project management and coordination. 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 <u>section 6.4</u>.

<sup>&</sup>lt;sup>2</sup> In this fourth DEFRA call and in deviation of the rules of the previous DEFRA calls, private non-private research centres can be coordinator of a proposal.

<sup>&</sup>lt;sup>3</sup> DLD and MHQA must inform the RMA of all proposals they are participating in.

- 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.
- Chair all meetings of the Steering Committee, unless decided otherwise in a meeting of the Steering Committee.
- 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.

#### 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.

#### 3.6. RESEARCH ETHICS

The first code of ethics for scientific research in Belgium was drawn up in 2009 (see <a href="http://www.belspo.be/belspo/organisation/publ/pub\_ostc/Eth\_code/ethcode\_en.pdf">http://www.belspo.be/belspo/organisation/publ/pub\_ostc/Eth\_code/ethcode\_en.pdf</a>).

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, with the support of BELSPO.

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.

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

# 3.7. BUDGET RULES

**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:

- 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 for LargeCap enterprises, maximum 75% for MidCap and 80% for SME. The remaining % is indicated in the proposal as the partner contribution.

|                                       | Public Research Institute and Private non-profit research centre | Private company   |
|---------------------------------------|--|---|
| Partner budget<br>FINANCED BY DEFENCE | • 100% eligible costs  | <ul> <li>LargeCap enterprises: 65% eligible costs</li> <li>MidCap enterprises: 75% eligible costs</li> <li>SME: 80% eligible costs</li> </ul> |

To discriminate between SME, MidCap and LargeCap enterprises article 2 of <u>Regulation (EU) 2021/697 of the</u> <u>European Parliament and of the Council of 29 April 2021 establishing the European Defence Fund and repealing</u> <u>Regulation (EU) 2018/1092</u> is applied, which refers to Article 2 of the <u>Annex to Commission Recommendation</u> <u>2003/361/EC.</u>

|                                    | Article 2 of Regulation (EU) 2021/697 of the European Parliament and of the Council of 29 April 2021 establishing the European Defence Fund and repealing Regulation (EU) 2018/1092 is applied, which refers to Article 2 of the <u>Annex to Commission</u> <u>Recommendation 2003/361/EC</u>   |
|------------------------------------|---|
| SME – Small and Medium Enterprises | Staff headcount and financial ceilings determine enterprise categories within the SMEs:<br>1. The category of micro, small and medium-sized enterprises (SMEs) is made up of enterprises which employ fewer than 250<br>persons and which have an annual turnover not exceeding EUR 50 million, and/or an annual balance sheet total not exceeding<br>EUR 43 million.<br>2. Within the SME category, a small enterprise is defined as an enterprise which employs fewer than 50 persons and whose annual<br>turnover and/or annual balance sheet total does not exceed EUR 10 million.<br>3. Within the SME category, a microenterprise is defined as an enterprise which employs fewer than 10 persons and whose annual<br>turnover and/or annual balance sheet total does not exceed EUR 2 million. |
| MidCap Enterprises                 | 'Middle capitalisation company' or 'mid-cap' means an enterprise that is not a SME and that employs a maximum of 3 000 persons, where the headcount of staff is calculated in accordance with Articles 3 to 6 of the Annex to Recommendation 2003/361/EC.   |
| LargeCap Enterprises               | The 'large-cap' enterprises employ more than 3 000 persons, where the headcount of staff is calculated in accordance with Articles 3 to 6 of the Annex to Recommendation 2003/361/EC.   |

In the full proposal (section 6.5 Budget assessment) the total project budget should be detailed in the tables (100% cost). 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.

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.

For persons not identified by name in the proposal, the staff costs are limited to a maximum amount of:

- 5 400 €/month FTE for a technician/bachelor (regardless of years of experience)
- 7 600€/month FTE for a Master (regardless of years of experience)
- 8 300 €/month FTE for a Master in engineering (regardless of years of experience)
- 10 000€/month FTE for a PhD (regardless of years of experience)

The RHID only accepts staff to be hired under a labour contract. Tax-free doctoral or post-doctoral scholarships are not accepted.

**General operating costs**: this includes daily/usual supplies and products for the laboratory, workshop and office, documentation, consignments, use of daily software and IT facilities, organisation of internal meetings, etc. 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 strictly related to the project, even if supporting documents are not requested. Although no detailed justification is required for these costs, the administration of the concerned partner must keep these invoices in its accounts in the event of an audit.

**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, 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.

**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<br>(monthly costs)     | GENERAL<br>OPERATION COSTS                              | SPECIFIC<br>OPERATION<br>COSTS | OVERHEADS   | EQUIPMENT | SUBCONTRACTING                                     |
|-------------|------------------------------------|---|--------------------------------|---|-----------|--|
| ATOR        | Technician: 5 400€/month           | <br>15% of Staff costs<br>(Automatically<br>generated)  | -                              | 10% of [Staff costs +<br>Operation costs]<br>(Automatically<br>generated) | -         | Max. 25% of the<br>total budget of<br>this partner |
| COORDINATOR | Master: 7 600€/month               |   |                                |   |           |  |
|             | Master (engineering): 8 300€/month |   |                                |   |           |  |
| PROJECT     | <b>PhD:</b> 10 000€/month          |   |                                |   |           |  |
| PARTNERS    | Technician: 5 400€/month           | -<br>10% of Staff costs<br>(Automatically<br>generated) | -                              | 10% of [Staff costs +<br>Operation costs]<br>(Automatically<br>generated) | -         | Max. 25% of the<br>total budget of<br>this partner |
|             | Master: 7 600€/month               |   |                                |   |           |  |
| PROJECT     | Master (engineering): 8 300€/month |   |                                |   |           |  |
| OTHER       | <b>PhD:</b> 10 000€/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 DEFRA on-line submission platform:

# https://defra.belspo.be

#### 4.1. PHASE 1 – PRE-PROPOSAL

A **pre-proposal** must be submitted at the latest on **22 February 2024 (14h00).** If the pre-proposal has not been submitted in time, it will be impossible to submit a full proposal.

The following information needs to be filled in directly into the online platform:

- The choice of the theme
- The title and acronym of the project
- The coordinates of the foreseen partners
- Summary of the project (1/2 page)
- Keywords (min 2; max 6).
- The name and contact details of 4 to 6 scientific experts (minimum **2 Belgian** and **2 foreign** experts) capable of assessing the proposal. The proposed experts must comply with the eligibility criteria for remote experts see <u>'Evaluators eligibility'</u>.
- Optionally, the name and contact details of 2 non-grata scientific experts to be excluded from the evaluation of the proposal under the condition of sufficient motivation.

The pre-proposal form can be downloaded from the platform and will contain:

- The title and acronym of the project.
- The choice of the theme.
- The coordinates of the foreseen partners.
- A brief description of the intended project: the scope, objectives, the innovation with respect to the state of the art, the relevance and potential impact of the project for Defence.
- Relevant references of the partners in relation to the project, incl. a short profile of the foreseen partners and a description of the added value of the partnership in addressing the research topic.

The total length of the **pre-proposal** should not exceed 9 **pages** format A4.

Companies, a(i)sbl and foundations must upload the extract of the Ultimate Beneficial Owner (UBO) register as an annex to the pre-proposal (in pdf format).

Besides the extracts of the Ultimate Beneficial Owner (UBO), no other annexes are allowed.

The pre-proposals will be evaluated by an internal evaluation committee of the Belgian Defence (see <u>section</u> 5.1.1.).

On 14 March 2024, the internal evaluation committee will invite for each pre-defined theme (themes 1 to 5) maximum five (5) pre-proposals to submit a full proposal.
 Only for theme 6, "open call: Research on Innovative and Future-oriented Defence Solutions" maximum ten (10) pre-proposals will be invited to submit a full proposal.

The pre-proposals will also be used by BELSPO and the RHID to seek experts for the evaluation of the full proposals.

# 4.2. PHASE 2 - FULL PROPOSAL

For the themes 1, 2, 3, 4 and 5, maximum five (5) pre-proposals will be invited to submit a full proposal. For theme 6, maximum ten (10) pre-proposals will be invited to submit a full proposal. Applicants must submit the full proposal via the online DEFRA submission platform.

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. 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) register to the call secretariat by e-mail to defra@belspo.be.

The **full proposal** must be submitted at the latest on **18 April 2024 (14h00).** If the full proposal does not comply with the submission rules or has not been submitted in time, it will not be taken into account for evaluation.

#### Content of the full proposal:

Within the full proposal form:

- The title, acronym and summary of the project.
- The name and contact details of the project partner(s).
- The proposal description:
  - scope and objectives,
  - o state of the art and innovative character,

- o relevance and potential impact for Defence, including the data management plan,
- o quality of the partners/partnership of the project,
- o coherence between research objectives and methodology,
- the work plan: work packages, the project risk assessment, the budget assessment.

As a separate form:

- The GANTT chart (mandatory)
- Cash or in-kind commitment letter (not mandatory)

# 5. EVALUATION PROCEDURE AND CRITERIA

#### 5.1. EVALUATION PROCEDURE

5.1.1. PHASE 1 – EVALUATION OF PRE-PROPOSALS

Only pre-proposals that are complete and submitted in time will be taken into account.

The pre-proposals will be evaluated by an internal evaluation committee of the Belgian Defence on the basis of the following criteria:

- The correspondence of the pre-proposal with the scope of the call themes
- The quality of the pre-proposal, based on the description of the project objectives and the innovation with respect to the state of the art
- The quality of the partners and the adequacy of the partnership.
- The relevance and potential impact for Defence.

More information about the criteria used can be found in the <u>evaluation matrix for pre-proposals</u>.

The RHID will translate the outcome of each pre-proposal's evaluation into numeric scores. In practice, this will be done as follows:

- 1. Translating the appreciations given to each sub-criterion into scores.
- 2. Adding the scores of the sub-criteria to obtain a total for each criterion.
- 3. Performing a weighted sum of the criteria in the following way:

| WEIGHT OF THE DIFFERENT CRITERIA                      | THEMEs 1, 2, 3, 4, 5 | THEME 6 |
|---|----------------------|---------|
| Quality of the pre-proposal                           | 40%                  | 30%     |
| Quality of the partners & Adequacy of the partnership | 30%                  | 30%     |
| Impact  | 30%                  | 40%     |

According to the scores obtained, the proposals will be ranked in a list per theme (Pre-proposal Ranking). For the pre-proposals submitted in themes 1, 2, 3, 4 and 5, this list will serve as the base for the selection of the applicants invited to introduce a full proposal.

For the pre-proposals submitted in the open theme 6, the internal evaluation committee of the Belgian Defence can apply additional criteria based on strategic considerations and the diversity of topics of the pre-proposals.

This evaluation will take place within three weeks after the submission of the pre-proposals. On **14 March 2024**, BELSPO will communicate the conclusions of the internal evaluation committee to the applicants and will invite the selected pre-proposals to submit a full proposal.

# 5.1.2. PHASE 2 – EVALUATION OF FULL PROPOSALS

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

The selection of 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

#### STEP 1 - REMOTE SCIENTIFIC PEER REVIEW EVALUATION

BELSPO 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 3 independent experts having an adequate combined expertise to evaluate the research proposal. Each expert team will be composed of minimum one Belgian and minimum one foreign expert.

BELSPO is responsible for composing this remote 'written evaluation team' with experts from BELSPO's and RHID's own databases and experts suggested by the applicants.

For each proposal, an individual written evaluation is performed. The written evaluation takes place remotely, via the online DEFRA evaluation platform, 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 a variety of (sub)criteria, namely in the following categories:

- Scientific quality
- Quality and efficiency of the implementation
- Impact

More information about the criteria used can be found in the evaluation matrix for full proposals.

Once all written evaluations have been introduced for a given proposal, the evaluations reports will be compiled into a Consensus Report for each proposal. The Consensus Report will consist of appreciations and comments for the different (sub)criteria.

The report will also include questions to which the applicants must **respond in writing** prior to the presentation to the Scientific Expert Committee (SEC) (step 2).

At this stage, the Consensus Reports are definitive. They will not be modified in the subsequent steps of the evaluation.

The individual evaluations are neither communicated to the Scientific Expert Committees, nor to the applicants.

On **21 June 2024**, applicants will get access to an anonymised version of their definitive Consensus Report, in preparation of the presentation for the SEC. They will also get the list of questions to which they must answer in writing by **26 July 2024**.

STEP 2 – SCIENTIFIC EXPERTS COMMITTEE EVALUATION, INCLUDING INTERVIEWS WITH THE APPLICANTS

Preparation of the Scientific Experts Committee (SEC) evaluation

BELSPO will translate the outcome of each proposal's evaluation into numeric scores. In practice, this will be done as follows:

- 1. Translating the appreciations given to each sub-criterion into scores.
- 2. Adding the scores of the sub-criteria to obtain a total for each criterion.
- 3. Performing a weighted sum of the criteria in the following way:

| WEIGHT OF THE DIFFERENT CRITERIA             | ALL THEMES |  |
|--|------------|--|
| Scientific quality                           | 35%        |  |
| Quality and efficiency of the implementation | 40%        |  |
| Impact                                       | 25%        |  |

According to the scores obtained, 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 receive the corresponding Proposal Rankings, and will have access, via the online DEFRA evaluation platform, to the proposals as well as the anonymised Consensus Reports. The Consensus Reports shall not be modified by the SEC.

Each SEC will organise interviews<sup>4</sup> with the applicants of the full proposals according to the following schedule:

- Presentation by the applicants, including an introduction of the proposal and integrating the answers to the questions of the remote experts (15 minutes).
- Questions and answers (Q&A) (15 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 specific criteria:

- Budget availability.
- Complementarities and/or overlaps between proposals.
- The coherence of the proposals with the strategic objectives (scope) of the themes.
- The cohesion of the partnership.
- General appreciation of the presentation by the applicants.

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 preference for funding.

# STEP 3 - SELECTION PROPOSAL FORMULATED BY THE SCIENTIFIC COMMITTEE OF THE RHID

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
- Full proposal and Consensus Report of each proposal (on demand)

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.

<sup>&</sup>lt;sup>4</sup> Physical meeting if possible - online meeting if necessary. Detailed instructions to adequately prepare the panel presentation will be sent separately.

The Scientific Committee will formulate the Scientific Committee Funding Scenario taking into account the following rules:

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

#### 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.

#### 5.2. EVALUATION CRITERIA

The evaluation criteria that are used in each step of the evaluation procedure are described in the evaluation matrices (pre- and <u>full</u> proposal).

#### 6. CONTRACTUAL OBLIGATIONS FOR SELECTED PROJECTS

#### 6.1. PROJECT STARTING AND END DATE

The projects selected within the context of the current call will start in December 2024.

The project contracts will have a duration of 2 to maximum 4 years (plus 3 months to allow meeting all administrative requirements before the effective start-up of the project).

#### 6.2. CONTRACTS

For the selected proposals, a contract is concluded 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 2024 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.

This Annex I will be drawn up in consultation between the funded partners of the selected proposals and the Belgian Defence/RHID. Recommendations formulated by the evaluators and the Scientific Committee will be taken into account when drafting the Technical specifications (Annex I).

Adaptations to the original proposal may relate, among other things, to the content of the research, the composition of the project partnership, the budget, the proposals for valorising the research.

## Annex I "Technical specifications" is signed by the DEFRA programme manager and the promotors concerned.

<u>Annex II "General conditions applicable to the contract"</u> contains all general provisions applicable to all DEFRA contracts. Annex II is the same for all DEFRA projects of a specific call. It is available on the DEFRA 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.

In case a "Cash or in-kind commitment letter" is associated to the selected project, this commitment and contribution will be formalised by means of a bilateral contract between the external partner(s) and the project partner(s). The bilateral contract shall be in conformity with all the provisions contained in the DEFRA project contract. The provisions of the bilateral contract shall always be subordinate to the provisions of the DEFRA contract. A copy of the bilateral contract must be handed over to the Royal Higher Institute for Defence (RHID, defra@mil.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 of Belgian Defence.

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 year to discuss the project's progress. The organisation of such meeting must be included in the project work plan and the project budget. Ideally, this(these) meeting(s) should take place in the same period as the delivery of the progress report(s).

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. REPORTS

The contract foresees the following reports to be submitted to the RHID:

- Initial report: to be submitted within three months after 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 three months 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.

#### 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.

#### 7.2. SPECIFIC CONDITIONS

For social and humanities data, a copy of the data and/or metadata can be transferred to SODHA (Social Sciences and Digital Humanities Archive) (<u>https://www.sodha.be</u>) after explicit approval of RHID.

#### 7.3. CLASSIFIED INFORMATION/SECURITY RELATED ACTIVITIES

Certain activities undertaken in the frame of the projects may use or generate classified information. This paragraph solely concerns protective measures to be taken to preserve the confidentiality of security-sensitive information regarding these research 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 11 Dec 1998 Art 3/Loi du 11 Déc 1999 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 taking into account both 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 Full-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 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) <u>https://www.nvoans.be/</u>

This security analysis will not be part of the evaluation process but is essential to be able to start the project.

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

Both BELSPO and RHID place great importance on the quality of their service and on improving the way they operate. A complaint about the administrative handling of this call for proposals will be handled by BELSPO, RHID will handle complaints about the 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 at the following address: <u>http://www.belspo.be/belspo/organisation/complaints\_en.stm</u>

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 the **secretariat**: defra@belspo.be