European Defence Fund (EDF)

Call for proposals

EDF-2022-DA

Version 1.0
09 June 2022

HISTORY OF CHANGES			
Version	**Publication Date**	**Change**	**Page**
1.0	09.06.2022	– Initial version.	
		–	
		–	
		–	

EUROPEAN COMMISSION
Directorate-General for Defence Industry and Space

DEFIS.A – Defence Industry

CALL FOR PROPOSALS

TABLE OF CONTENTS

0. Introduction

This is a call for proposalsfor EU **action grants** in the field of collaborative defence research and development under the **European Defence Fund (EDF)**.

The regulatory framework for this EU Funding Programme is set out in:

- Regulation 2018/1046 (EU Financial Regulation)
- the basic act (EDF Regulation 2021/697[1]).

The call is launched in accordance with the Work Programmes 2022 Part II[2] and 2023 Part I[3] and will be managed by the **European Commission, Directorate-General for Defence Industry and Space (DG DEFIS)**.

The call covers the following **12 topics**:

- **EDF-2022-DA-C4ISR-EC2: European command and control system**
- **EDF-2022-DA-C4ISR-SOFC2: Deployable special operations forces multi-environment command post and C2 System**
- **EDF-2022-DA-CYBER-CIWT: Cyber and information warfare toolbox**
- **EDF-2022-DA-CYBER-CSIR: Cybersecurity and systems for improved resilience**
- **EDF-2022-DA-SPACE-ISR: Innovative multi-sensor space-based Earth observation capabilities towards persistent and reactive ISR**
- **EDF-2022-DA-SPACE-SBMEW: Space-based missile early warning**
- **EDF-2022-DA-MATCOMP-SMT: Smart and multifunctional textiles**
- **EDF-2022-DA-AIR-AEW: Airborne electronic warfare**
- **EDF-2022-DA-GROUND-CGC: Collaborative combat for land forces**
- **EDF-2022-DA-NAVAL-MSAS: Medium-size semi-autonomous surface vessel**
- **EDF-2022-DA-NAVAL-NCS: Naval Collaborative Surveillance**
- **EDF-2022-DA-SIMTRAIN-MSSI: Modelling, simulation and simulator integration contributing to decision-making and training**

Each project application under the call must address only one of these topics. Applicants wishing to apply for more than one topic, must submit a separate proposal under each topic.

We invite you to read the **call documentation** carefully, and in particular this Call Document, the Model Grant Agreement, the EU Funding & Tenders Portal Online Manual and the EU Grants AGA — Annotated Grant Agreement.

[1] 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 (OJ L 170, 12.5.2021).

[2] Commission Implementing Decision C(2022) 3403 final of 25/05/2022 on the financing of the European Defence Fund established by Regulation (EU) No 2021/697 of the European Parliament and the Council and the adoption of the work programme for 2022 - Part II.

[3] Commission Implementing Decision C(2022) 3659 final of 07/06/2022 on the financing of the European Defence Fund established by Regulation (EU) No 2021/697 of the European Parliament and the Council and the adoption of the work programme for 2023 - Part I.

These documents provide clarifications and answers to questions you may have when preparing your application:

- the Call Document outlines the:
  - background, type of action and funding rate, objectives, scope and types of activities, functional requirements, expected impact and specific topic conditions (sections 1 and 2)
  - timetable and available budget (sections 3 and 4)
  - admissibility and eligibility conditions, including mandatory documents (sections 5 and 6)
  - criteria for financial and operational capacity and exclusion (section 7)
  - evaluation and award procedure (section 8)
  - award criteria (section 9)
  - legal and financial set-up of the Grant Agreements (section 10)
  - how to submit an application (section 11)
- the Online Manual outlines the:
  - procedures to register and submit proposals online via the EU Funding & Tenders Portal ('Portal')
  - recommendations for the preparation of the application
- the AGA — Annotated Grant Agreement contains:
  - detailed annotations on all the provisions in the Grant Agreement you will have to sign in order to obtain the grant *(including cost eligibility, payment schedule, accessory obligations, etc)*.

You are also encouraged to visit the DG DEFIS webpage to consult the list of projects funded previously.

1. Background

The European Defence Fund (EDF) fosters the competitiveness, efficiency and innovation capacity of the European defence technological and industrial base (EDTIB).

It contributes to the EU strategic autonomy and its freedom of action, by supporting collaborative actions and cross-border cooperation between legal entities throughout the Union, in particular SMEs and mid-caps, as well as by strengthening and improving the agility of both defence supply and value chains, widening cross-border cooperation between legal entities and fostering the better exploitation of the industrial potential of innovation, research and technological development, at each stage of the industrial lifecycle of defence products and technologies.

The EDF funds projects which are consistent with the defence capability priorities commonly agreed by EU Member States within the framework of the Common Foreign and Security Policy (CFSP), through:

- collaborative research that could significantly boost the performance of future capabilities, aiming to maximise innovation and introduce new defence products and technologies, including disruptive technologies for defence, and aiming to make the most efficient use of defence research spending in the EU

or

- collaborative development of defence products and technologies, thus contributing to the greater efficiency of defence spending in the EU, achieving greater economies of scale, reducing the risk of unnecessary duplication and thereby fostering the market uptake of European defence products and technologies and reducing the fragmentation of defence products and technologies, ultimately leading to an increase in the standardisation of defence systems and a greater interoperability between Member States' capabilities.

In line with the EDF Work Programmes 2022 Part II and 2023 Part I, this call covers the thematic topics addressing development actions to be implemented through actual costs grants.

2. Type of action and funding rate — Objectives — Scope and types of activities — Functional requirements — Expected impact — Specific topic conditions

Type of action and funding rate

The topics under this call for proposals concern EDF Development Actions (DA).

For Development Actions, the IT system *(e.g. budget table in the Submission System, payment calculator in the Grant Management System)* will for technical reasons display a general funding rate of 100% for all automated calculations.

In order to calculate the rates that are due under the EDF Regulation, you will have to calculate the individual funding rates for your project (via the Detailed budget table available in the Submission System, *see section 5*).

These rates will be based on the:

- baseline funding rates (per type of activity)

and

- bonuses (per type of activity and depending on type of participants, if any).

Types of activities *(art 10(3) EDF Regulation)*		**Baseline funding rate**	**PESCO bonus**	**SME bonus**		**Mid-cap bonus**	**Maximum funding rate with bonuses**
				non-cross-border	**cross border**		
(a)	Activities that aim to create, underpin and improve knowledge, products and technologies, including disruptive technologies, which can achieve significant effects in the area of defence (**generating knowledge**)	*Cannot be funded*	*Cannot be funded*	*Cannot be funded*	*Cannot be funded*	*Cannot be funded*	*Cannot be funded*

(b)	Activities that aim to increase interoperability and resilience, including secured production and exchange of data, to master critical defence technologies, to strengthen the security of supply or to enable the effective exploitation of results for defence products and technologies (**integrating knowledge**)	65%	+ 10%	+ X% *(see table below)*	+ X% *(see table below)*	+ 10%	up to 100%
(c)	**Studies**, such as feasibility studies to explore the feasibility of new or upgraded products, technologies, processes, services and solutions	90%	+ 10%	+ X% *(see table below)*	+ X% *(see table below)*	+ 10%	up to 100%
(d)	**Design** of a defence product, tangible or intangible component or technology as well as the definition of the technical specifications on which such a design has been developed, including any partial test for risk reduction in an industrial or representative environment	65%	+ 10%	+ X% *(see table below)*	+ X% *(see table below)*	+ 10%	up to 100%
(e)	**System prototyping**[4] of a defence product, tangible or intangible component or technology	20%	+ 10%	+ X% *(see table below)*	+ X% *(see table below)*	+ 10%	up to 55%
(f)	**Testing** of a defence product, tangible or intangible component or technology	45%	+ 10%	+ X% *(see table below)*	+ X% *(see table below)*	+ 10%	up to 80%
(g)	**Qualification**[5] of a defence product, tangible or intangible component or technology	70%	+ 10%	+ X% *(see table below)*	+ X% *(see table below)*	+ 10%	up to 80%
(h)	**Certification**[6] of a defence product, tangible or intangible component or technology	70%	+ 10%	+ X% *(see table below)*	+ X% *(see table below)*	+ 10%	up to 80%
(i)	Development of technologies or assets **increasing efficiency** across the life cycle of defence products and technologies	65%	+ 10%	+ X% *(see table below)*	+ X% *(see table below)*	+ 10%	up to 100%

In order to obtain the bonuses, the applicants must fulfil the following conditions:

[4] 'System prototype' means a model of a product or technology that can demonstrate performance in an operational environment.

[5] 'Qualification' means the entire process of demonstrating that the design of the product, component or technology meets the specified requirements, providing objective evidence by which particular requirements of a design are demonstrated to have been met.

[6] 'Certification' means the process by which a national authority certifies that the product, component or technology complies with the applicable regulations.

Type of bonus	**Condition**	**Bonus** *(additional number of percentage points to the baseline funding rate)*
PESCO bonus	Project developed in the context of a project of the permanent structured cooperation (PESCO)[7]	+ 10%
SME[8] bonus (non-cross border)	Proportion of eligible costs allocated to SMEs (beneficiaries, affiliated entities and subcontractors involved in the action; not associated partners) ≥ 10% (for the activity concerned)	+ % of the proportion of eligible costs allocated to non-cross-border SMEs[9] (up to maximum 5%)
SME bonus (cross-border)		+ twice the % of the proportion of eligible costs allocated to cross-border SMEs[10]
Mid-cap bonus	Proportion of eligible costs allocated to mid-caps[11] (beneficiaries, affiliated entities and subcontractors involved in the action; not associated partners) ≥ 15% (for the activity concerned)	+ 10%

⚠ Please note that only entities which are registered in the Participant Portal (i.e. have a PIC) and which have a positive SME/Mid-cap self-assessment result (for the current and 2 previous years) can be counted for the SME/Mid-cap bonuses. Please make sure that all your project participants fulfil these requirements (Funding & Tenders Portal account > My Organisations > Actions > Modify Organisation > SME tab > Start SME self-assessment (> Mid-cap self-declaration); for more information, *see IT How To*).

⚠ Please also note that for WP 1 — Project management and coordination, you must always use the funding rate for the type of activity (c) Studies.

The funding rates that will cap the maximum amounts that may be requested for each applicant and reporting period will then be fixed in Annex 2e of the Grant Agreement.

Specific topic conditions

- For all topics under this call, multi-beneficiary applications are mandatory and specific conditions for the consortium composition apply *(see section 6)*

- For all topics under this call, following reimbursement option for equipment costs applies: depreciation and full cost for listed equipment *(see section 10)*

[7] See Council Decision (CFSP) 2017/2315 of 11 December 2017 establishing permanent structured cooperation (PESCO) and determining the list of participating Member States (OJ L 331, 14.12.2017, p. 57).

[8] 'SMEs' means small and medium-sized enterprises as defined in the Annex to EU Recommendation 2003/361/EC.

[9] 'Non-cross-border SMEs' are SMEs established in the Member States or EDF associated countries in which the beneficiaries that are not SMEs are established.

[10] 'Cross-border SMEs' are SMEs established in Member States or EDF associated countries other than those in which the beneficiaries that are not SMEs are established.

[11] 'Middle-capitalisation company (mid-cap)' means an enterprise that is not an SME and that has up to 3 000 employees, where the staff headcount is calculated in accordance with Articles 3 to 6 of the Annex to EU Recommendation 2003/361/EC.

EDF-2022-DA-C4ISR-EC2: European command and control system

Objectives

General objective

An effective and robust EU military C2 capability for missions and operations is an essential element of the overall EU effort regarding the CSDP. The lack of an adequate Joint C2 system in the EU military C2 structure is a critical shortfall identified in the EU High Impact Capability Goals 2020 and capability development processes in the area of cross-domain capabilities contributing to achieve EU's Level of Ambition (LoA), particularly, capabilities to operate autonomously within EU's LoA. This is especially pressing for the development of the Military Planning and Conduct Capability (MPCC), which is currently not able to achieve the Full Operational Capable status with the current C2 and CIS arrangements. Interoperability with existing or in-development national C2 systems is of key importance in order to ensure the seamless coordination of joint and combined (EU) military operations.

Specific objective

This call for proposals intends to pave the way for complementing or replacing existing European External Action Service (EEAS) C2 and Communication and Information Systems (CIS), to enhance and further develop the Military Planning and Conduct Capability (MPCC), covering all military operations, both executive and non-executive, within the EU's Level of Ambition as formulated in the EU Global Strategy, subsequent Council Conclusions and the Strategic Compass. The ultimate aim is to allow planning and conduct of CSDP missions and operations at strategical and operational level.

Considering the MPCC development timescale and other relevant documents, such as the Strategic Compass, the action must be finalised, in accordance with the requirements contained in this call, by the end of 2025.

Scope and types of activities

Scope

Proposals must demonstrate the capability to develop such a C2 capability and business and common services using a software technology model. Interfaces with existing and in-development EU, NATO and national C2 systems must be substantiated to ensure future interoperability.

The software technology model, which may integrate existing modules, must provide the services and functionalities required to demonstrate that the MPCC, as the main foreseen end-user, would be able to simultaneously plan and conduct executive and non-executive missions and operations, anywhere in the world, autonomously or in cooperation with other EEAS services, EU Member States, Norway or international organizations (*e.g.,* mainly NATO).

The demonstration of the software technology model should be based on a scenario with the mandatory participation of the MPCC as the main foreseen end-user and include the end-to-end connections and business exchanges with national C2 systems required for seamless command and control at EU-level in close coordination and collaboration with national authorities.

This demonstrated software technology model should pave the way for any further required developments and allow EU to launch the procurement of a new C2 capability eventually, including regarding the C2 software suite components that should be ready, and include the necessary provisions, to allow the end-user a fast and agile transition from software delivery to operational use.

Potential synergies and complementarity with ongoing projects at national, multinational, or EU level in particular, must be given due consideration. In any case, proposals must not duplicate the main objective and work requested in the call EDIDP-ESC2S-2019 – *European Command and Control (C2) system for strategic and operational level*[12].

Types of activities

The following table lists the types of activities which are eligible, and whether they are mandatory or optional *(see Article 10(3) EDF Regulation)*:

Types of activities (art 10(3) EDF Regulation)		**Eligible?**
(a)	Activities that aim to create, underpin and improve knowledge, products and technologies, including disruptive technologies, which can achieve significant effects in the area of defence (**generating knowledge**)	No
(b)	Activities that aim to increase interoperability and resilience, including secured production and exchange of data, to master critical defence technologies, to strengthen the security of supply or to enable the effective exploitation of results for defence products and technologies (**integrating knowledge**)	Yes (optional)
(c)	**Studies**, such as feasibility studies to explore the feasibility of new or upgraded products, technologies, processes, services and solutions	Yes (optional)
(d)	**Design** of a defence product, tangible or intangible component or technology as well as the definition of the technical specifications on which such a design has been developed, including any partial test for risk reduction in an industrial or representative environment	Yes (mandatory)
(e)	**System prototyping**[13] of a defence product, tangible or intangible component or technology	Yes (optional)
(f)	**Testing** of a defence product, tangible or intangible component or technology	Yes (optional)
(g)	**Qualification**[14] of a defence product, tangible or intangible component or technology	Yes (optional)
(h)	**Certification**[15] of a defence product, tangible or intangible component or technology	Yes (optional)
(i)	Development of technologies or assets **increasing efficiency** across the life cycle of defence products and technologies	Yes (optional)

[12] https://ec.europa.eu/info/funding-tenders/opportunities/portal/screen/opportunities/topic-details/edidp-esc2s-2019.

[13] 'System prototype' means a model of a product or technology that can demonstrate performance in an operational environment.

[14] 'Qualification' means the entire process of demonstrating that the design of the product, component or technology meets the specified requirements, providing objective evidence by which particular requirements of a design are demonstrated to have been met.

[15] 'Certification' means the process by which a national authority certifies that the product, component or technology complies with the applicable regulations.

Among mandatory design activities, initial tests and delivery of the software technology model to be developed should be attained within two years after the signature of the grant agreement.

Moreover:

- projects addressing activities referred to in point (d) above must be based on harmonised defence capability requirements jointly agreed by at least two Member States or EDF associated countries (or, if studies within the meaning of point (c) are still needed to define the requirements, at least on the joint intent to agree on them)
- projects addressing activities referred to in points (e) to (h) above, must be:
  - supported by at least two Member States or EDF associated countries that intend to procure the final product or use the technology in a coordinated manner, including through joint procurement

  and

  - based on common technical specifications jointly agreed by the Member States or EDF associated countries that are to co-finance the action or that intend to jointly procure the final product or to jointly use the technology

  (or, if design within the meaning of point (d) is still needed to define the specifications, at least on the joint intent to agree on them).

Functional requirements

The capability to be developed should meet the following functional requirements:

REQ 1 - High degree of reliability and availability.

REQ 2 - High level of maturity that paves the way for the end user’s swift transition from software delivery to operational use.

Software operational functionalities:

REQ 3 - Plans:

- Web Based Planning for planning operations/missions. Highly flexible and based on open workflows of information and templates.
- Operations Planning. Support. Specification of actors, timings, objectives to achieve the campaign goals; designing and comparing Courses Of Actions (COA), producing the Synchronization matrix; ROE management.
- Integration of common services (GIS, Messaging, data distribution, etc.), applied to planning.

REQ 4 - Cyber activities and Cyber operations:

- Recognized Cyber Picture (RCyP): Integrate and disseminate available cyber information into the operational to achieve Real-time full Cyber Situational Awareness.
- Rapid defensive response: Rapid containment and response to cyber-attacks.
- Cyber risks management: Cyber risks management during the planning and execution phases of an operation considering and evaluating known threats, risks and information from intelligence sources and the Cyber Space Situation.

REQ 5 - Intelligence, Surveillance and Reconnaissance (ISR):

- Advanced Intelligence Exploitation to collect, process and analyse a wide range of data types (video, imagery, reports, office documents) from open sources and generating different types of analysis view (relational diagrams, temporal, statistical…). It includes advanced search and analysis capabilities on structured and non-structured data.
- Monitoring and assessing international events to detect potential risks.
- Early Warning and SA to have a clear view of the monitored areas.
- Intelligence plans management. Collection plans and allocation of Intelligence, Surveillance & Reconnaissance (ISR) means.
- ORBAT[16] management.
- Comparison and extrapolation of own and adversary forces capabilities (based on equipment) with history enhanced.

REQ 6 - Missions and Operations**:**

- Missions/operations Assessment. Provide measurement of progress, effectiveness and results of the military missions/operations.
- Planning: measurable tasks, objectives, end state conditions, and associated effects and criterion to assist with assessing progress.
- Preparation & Execution: structured monitoring of the current situation and enables evaluation of the operation’s progress.
- Joint Task Force HQ Management. Support for the JTF HQ decision cycle and event management of Battle rhythm.
- Info Ops. Support for the analysis, planning, management, deployment, monitoring and assessment of coordinated military activities within the information domain.
- Battlespace management. To enable the dynamic coordination and synchronization of activities in the whole battlespace (Land, maritime, Air, Space, Cyber) according to the commander’s priorities.
- Situational Awareness. To gain knowledge, cognition and anticipation of events, factors and variables affecting the safe, expedient and effective conduct of missions/operations.
- Meteorological and Oceanographic (METOC) management. Provides information related to weather and oceanographic observation and forecasting.

REQ 7 - COP integration and management.

- Integration and management of the different COPs available: Recognized Air Picture (RAP), Recognized Maritime Picture (RMP), Recognized Civil Picture (RCP), Recognized Intelligence Picture (RIP), Recognized CIS Picture (RCISP), Recognized Logistics Picture (RLP), Recognized Electromagnetically Picture (REMP), Recognized Environmental Picture (REP), Recognized CRBN Picture (RCBRNP), Recognized Engineer Picture (RENGGP), Recognized Cyber Picture

[16] Order of battle report.

(RCyP), Recognized Medical Picture (RMedP), Recognized Targeting Picture, Space Domain Common Operating Picture (SCOP) and Other Partners Information.

REQ 8 - Logistics:

- Logistic information provision. Provide relevant and accurate logistic information related to EU and national forces and civilian actors timely.
- Infrastructure data management: Define and manage infrastructure objects like road and railway networks, airfields, ports, bridges or Reception, staging and Onward Movement (RSOM) hubs Ports of Debarkation (PODs).
- Force deployment planning. Calculate and plan convoy movements, and it will manage the resulting movement plans and resolve conflicts between activities during force deployment. It will find optimized paths in multi-modal transportation networks.
- Customs management. Generate required EU customs forms 302 and it will make use of EU existing or future projects that aim to digitize the EU customs form 302.

REQ 9 - Training**:**

- Initial capability for user training, simulation and exercises
- Management of Geographic Information System

REQ 10 - Core GIS:

- Cartography display and management, including access to ArcGIS server maps, with the ability to operate and convert all types of grids.
- Analysis and management of geospatial data.
- Symbology display and management compatible with relevant standards (APP-6A, APP-6B, APP-6C, APP-6D, MIL-STD-2525B and MIL-STD-2525C)
- Generation, management and display of automatic alarms and warnings based on geographic areas and track/contact lists.
- Use of Artificial Intelligence on both structured and unstructured data to collect, analyse and represent data.
- Geo Web Services: providing access to geographical data through common data exchange standards like Open Geospatial Consortium (OGC): Geography Markup Language (GML), Keyhole Markup Language (KML), Filter, Simple Features, Symbology Encoding, Web Feature Service (WFS), Web Map Service (WMS), Web Map Tile Service (WMTS) and Web Coverage Service (WCS).

REQ 11 - Interoperability:

- Process integration services allowing to integrate seamlessly with one another
- Data and information Exchange with import and export of data provided by current EU-systems to ensure the timely availability and integrity of information.
- Endless real-time data capacity (big data)

- Secure Office Local Area Network (SOLAN) that hosts EUCCIS and its successor (EC3IS).
- EUMS Lessons Management Application (ELMA)/ Collaboration Application for Management of EU-led Operations (CAMEO).
- Military Archiving and Retrieval System (MARS).
- Interoperability with different EU systems: EUMS Lessons Management Application (ELMA)/ Collaboration Application for Management of EU-led Operations (CAMEO), EU Operations Wide Area Network (EOW), RESCOM, MRC2.
- Interoperability with EU Member States and Norway systems based on common standards.
- Federated mission network (FMN) compliant.

REQ 12 - Common services.

- System administration and user management in line with relevant operational and security policies and doctrine.
- Provide e-mail exchange and common file network among EC2 users and with external entities.

Expected impact

The expected impacts from the action should be:

- Development of Joint C2 critical enablers for CSDP operations and missions.
- Reduction of the minimum reaction time for deployment of European military missions.
- Integration of all CIS and ISR data provided by Member States, Norway, EU forces, NATO and civil agencies.
- Situational awareness improvement, resilience and security of EU operations.
- Creation of a reference Strategic C2 System that will improve the capabilities of the European defence industry to develop and supply state-of-the-art C2 systems.
- Reinforcement of the interoperability of Member States and Norway' armed forces.
- Cost reduction of European military missions.
- Enhancement of unity of command, from the strategic to the tactical level.
- Interoperability achievement and matching of heterogeneous networks.
- Command connectivity improvement among all users.
- Visualization capabilities in near real time to multiple platforms and a broad range of capabilities and C&C-scenarios.
- Technological advancement concerning net centricity applied to military C4ISR systems.

EDF-2022-DA-C4ISR-SOFC2: Deployable special operations forces multi-environment command post and C2 System

Objectives

Symmetric and asymmetric threats inside and outside the EU territory require fast response and the ability to rapidly deploy transportable units implementing a Special Operations Forces Command Post and C2 System (SOFCPC2) to areas of interest, during both peace and wartime. The 2018 Capability Development Plan (CDP-2018) encodes this need in the priority "Cross-domain capabilities contributing to achieve EU's Level of Ambition" and in particular "c) Enabling capabilities to operate autonomously within EU's LoA" and more specifically: "Providing a deployable joint interoperable C2 capability readily available for integration so as to be able to operate more efficiently with international and regional partners."

General objective

In the context of CSDP operations, Small Joint Operations (SJO) conducted by Special Operation Forces (SOF) can provide a wide array of flexible military options for a rapid and effective response to the whole spectrum and all the stages of the fast-evolving crisis management landscape. The use of SOF can evidently decrease the risk of escalation that is generally associated with the employment of larger and more visible combat forces. Furthermore, SOF can be used in order to prepare and incorporate the full capacity and rapid deployment of such larger EU military forces and reinforce their operational capacities when they are already deployed in an operational theatre, in order to stabilise a deteriorating situation.

SOF can also contribute to the effort to maintain the maritime security across Mediterranean Sea, to conduct maritime security and interdiction operations in the context of combating maritime terrorist, to mitigate refugee flows and intercept illegal trafficking of people and goods.

Specific objective

A key contribution from SOF to SJO is their highly flexible mobility that can provide the ability to rapidly adapt and respond to a broad range of operational scenarios in every operational domain (land, sea, air and cyber) with minimum or no demand for host nation support.

Against this background, the SOFCPC2 should provide adequate flexibility, interoperability, deployability, scalability, discretion and redundancy, notably concerning communications systems and networks, in order to adapt easily in rapidly changing levels of conflict.

The duration of the proposed action shall not exceed three years and shall provide an initial operational capability of the prototype system.

Scope and types of activities

Scope

Proposals must focus on the development of a capability considering SOF specific requirements, which includes not only generic C2 capabilities but also those tailored for SOF. Those SOF specific requirements imply interoperability with higher level C2 Systems and with tactical edge communication systems for field deployed operators, rapid deployment capabilities in various areas of interest supporting several SOF teams, low thermal signature power supplies and multi-environment operational capabilities as a standalone asset.

Proposals must in particular address the development of:

- A SOFCPC2 hosting infrastructure, transportable by air, road and sea, and rapidly deployable, including accommodation facilities, HVAC[17], water supply and sewage to support all operations. The facilities should be modular and adaptable to all climate zones and in line with operating Member States and Norway' needs, with the ability to be deployed on board of sea-based assets or naval vessels.
- An autonomous, energy supply system with low thermal and acoustic emission that can be integrated to air, road and sea transportable SOFCPC2 hosting infrastructure.
- An ad-hoc, adaptive, interoperable, resilient, and cyber-secure, end-to-end SOFCPC2 communication system, able to be integrated in the broader C2 infrastructure, enabling the exchange of information across the entire command hierarchy, with platforms and down to the field-deployed operators.
- An integrated C2 platform, intelligence and sensing software platform.
- A system capable to receive and fuse information from heterogeneous sensors, manned and unmanned platforms.
- A SOFCPC2 end-user terminal (field-deployed special operator), including applications to achieve the integration of C2, intelligence, sensors, weapon systems and communications platforms to a seamless architecture.
- A SOFCPC2 perimeter security system and its integration with the C2 and communications platforms.

Types of activities

The following table lists the types of activities which are eligible, and whether they are mandatory or optional *(see Article 10(3) EDF Regulation)*:

Types of activities (art 10(3) EDF Regulation)		**Eligible?**
(a)	Activities that aim to create, underpin and improve knowledge, products and technologies, including disruptive technologies, which can achieve significant effects in the area of defence (**generating knowledge**)	No
(b)	Activities that aim to increase interoperability and resilience, including secured production and exchange of data, to master critical defence technologies, to strengthen the security of supply or to enable the effective exploitation of results for defence products and technologies (**integrating knowledge**)	Yes (optional)
(c)	**Studies**, such as feasibility studies to explore the feasibility of new or upgraded products, technologies, processes, services and solutions	Yes (mandatory)
(d)	**Design** of a defence product, tangible or intangible component or technology as well as the definition of the technical specifications on which such a design has been developed, including any partial test for risk reduction in an industrial or representative environment	Yes (mandatory)

[17] Heating Ventilation and Air Conditioning.

(e)	**System prototyping**[18] of a defence product, tangible or intangible component or technology	Yes (mandatory)
(f)	**Testing** of a defence product, tangible or intangible component or technology	Yes (mandatory)
(g)	**Qualification**[19] of a defence product, tangible or intangible component or technology	Yes (optional)
(h)	**Certification**[20] of a defence product, tangible or intangible component or technology	Yes (optional)
(i)	Development of technologies or assets **increasing efficiency** across the life cycle of defence products and technologies	Yes (optional)

Initial Operational Test and Evaluation (IOT&E) of the SOFCPC2 prototype must be attained within three years after the signature of the grant agreement.

The prototype of SOFCPC2 should be tested and evaluated for initial operational capability with facilities and equipment for multiple of ten of military personnel (at least 50), according to test scenarios and requirements that will be defined and provided by the operating Member States and associated countries before starting the design activities.

Functional requirements

The capability to be developed should meet the following functional requirements:

- REQ1 - The SOFCPC2 should provide a transportable by air, road and sea (sea-based assets, naval platforms and/or merchant vessels), able to be deployed in all climate zones and in line with operating Member States and associated countries' needs, with modular and rapidly deployable facilities, including HVAC, water supply, sewage, and energy supply systems to support its operations.

- REQ2 - The SOFCPC2 should implement a net–centric mobile ad hoc network with the ability to combine with heterogeneous networks of different architecture. It should integrate interoperable and cyber-secured communications at multiple levels enabling the exchange of information across the entire command hierarchy, between field-deployed SOF task groups and the SOFCPC2, within the SOFCPC2, from the SOFCPC2 towards higher hierarchical levels and from SOFCPC2 to close air supporting aircraft or other supporting units. For interoperability and compatibility purposes, the SOFCPC2 communication systems should take into account, as far as possible, all standards applicable to SOF operations, including those of NATO.

- REQ3 - The SOFCPC2 should feature all necessary software platforms related to the exercise of Command and Control (C2) of multiple SOF task groups operating concurrently in the field, including the generation of all necessary situation awareness to achieve that goal across multiple domains.

[18] 'System prototype' means a model of a product or technology that can demonstrate performance in an operational environment.

[19] 'Qualification' means the entire process of demonstrating that the design of the product, component or technology meets the specified requirements, providing objective evidence by which particular requirements of a design are demonstrated to have been met.

[20] 'Certification' means the process by which a national authority certifies that the product, component or technology complies with the applicable regulations.

- REQ4 - The SOFCPC2 should embody novel terminal devices with suitable SWaP characteristics for field deployed SOF task groups which must provide C2 functionality at the tactical edge in coordination with the SOFCPC2 C2 platform.

- REQ5 - The SOFCPC2 should feature a software platform providing Digitally Aided Close Air Support (DACAS) capability and able to share tactical on-site and other sources intelligence information for target detection, recognition and assignment, while making maximum use of interoperability standards.

- REQ6 - The SOFCPC2 should feature the relevant means to be integrated with several different aircraft and/or surface vessel platforms, manned and/or unmanned, employed either for the transportation of SOF Task Groups or for the collection of intelligence.

- REQ7 - The SOFCPC2 should feature a military grade, autonomous, horizontally scalable, and low thermal/acoustic signature power supply system capable of furnishing the energy needs of the entire SOFCPC2, employing a resilient and proactively managed mix of thermal and renewable sources and storage.

- REQ8 - The SOFCPC2 should feature a perimeter security system integrated with the core C2 and communications platforms, primarily passive and capable of detecting close range threats. The security system should be compliant with the overall SOFCPC2 electromagnetic spectrum.

- REQ9 - The SOFCPC2 should be modular and scalable in terms of facilities and equipment. Initially designed for deployments from 5 up to 150 military personnel, it should be expandable and upgradable to future operational capabilities while allowing integration of other additional modules and tools.

Expected impact

By providing a reference SOF C2 System, hence improving the capabilities of the European defence technological and industrial base to develop and supply state-of-the-art C2 systems, the action should contribute to:

- promote the upgraded role of SOF as envisioned by EU;

- enable efficient SOF deployments where no permanent C2 infrastructure exists, with a state-of-the-art deployable European SOFCPC2;

- shorten the response times of the EU and its Member States as well as associated countries during both peace and war time, for a variety of missions, both civilian and military;

- reduce the cost of EU SOF SJO missions;

- facilitate the collaboration and interoperability among Member States, notably through integrated CIS and ISR means provided by Member States and Norway, EU forces, and civil agencies;

- enhance the security of supply and reduce dependencies.

EDF-2022-DA-CYBER-CIWT: Cyber and information warfare toolbox

Objectives

General objective

The continuously and rapidly increasing flow of information in the information environment, facilitated through cyber capabilities, is a well-established fact. We are witnessing an increasing number of malicious actions targeting the information environment. In the more and more digitalized battlespace, the Cyber and Information domains become decisive to anticipate and manage conflicts in the full spectrum of threat activities from sub-threshold interference to open warfare.

Specific objective

Threats posed by new and evolving cyber and hybrid tools (e.g., disinformation, deep fakes) are fully part of Cyber and Information Warfare[21]. These threats need to be addressed with appropriate holistic resilience measures including detection and appropriate countermeasures. Cyber and Information Warfare system performance, in terms of total defence effectiveness and cooperation in cyber defence as referred in the EU Capability Development Plan Priorities, could be improved.

Scope and types of activities

Scope

Proposals are expected to address development of a European coherent library of software configurable components to easily integrate in Cyber and Information Warfare systems. This requires capabilities in detection, analysis, fusion and threat targeting to support activities of Cyber and Operational Centres for operational use cases (e.g., attacks against deployed forces in operations; attacks aiming to destabilize one and/or several European countries). Various relevant technologies processing multi-sources data for Cyber and Information Warfare operations needs to be addressed. In addition, enabling items such as standardization, data exchanges rules, multi-source fusion applications, AI-based analytics, methods & tools for integration, qualification in defence systems should be covered. The disinformation phenomenon includes also cultural and social aspects (so called "social science & humanity") that may be studied by multidisciplinary teams to provide a holistic perspective.

The outcome is expected to become both a reference repository of AI-based configurable applications and an experimental platform for the various AI techniques addressing the specificities of Cyber and Information Warfare (for example disinformation tracking applications).

Types of activities

The following table lists the types of activities which are eligible, and whether they are mandatory or optional *(see Article 10(3) EDF Regulation)*:

[21] https://www.nato.int/nato_static_fl2014/assets/pdf/2020/5/pdf/2005-deepportal4-information-warfare.pdf

Types of activities (art 10(3) EDF Regulation)		**Eligible?**
(a)	Activities that aim to create, underpin and improve knowledge, products and technologies*,* including disruptive technologies, which can achieve significant effects in the area of defence (**generating knowledge**)	No
(b)	Activities that aim to increase interoperability and resilience, including secured production and exchange of data, to master critical defence technologies, to strengthen the security of supply or to enable the effective exploitation of results for defence products and technologies (**integrating knowledge**)	Yes (optional)
(c)	**Studies**, such as feasibility studies to explore the feasibility of new or upgraded products, technologies, processes, services and solutions	Yes (optional)
(d)	**Design** of a defence product, tangible or intangible component or technology as well as the definition of the technical specifications on which such a design has been developed, including any partial test for risk reduction in an industrial or representative environment	Yes (mandatory)
(e)	**System prototyping**[22] of a defence product, tangible or intangible component or technology	Yes (mandatory)
(f)	**Testing** of a defence product, tangible or intangible component or technology	Yes (optional)
(g)	**Qualification**[23] of a defence product, tangible or intangible component or technology	Yes (optional)
(h)	**Certification**[24] of a defence product, tangible or intangible component or technology	Yes (optional)
(i)	Development of technologies or assets **increasing efficiency** across the life cycle of defence products and technologies	Yes (optional)

The proposals must include design and prototype activities. The proposal may include studies, testing, qualification, certification, and increasing efficiency activities.

The following tasks must be performed as part of the required activities:

(1) Define toolbox concept that enables the use/implementation of hardened AI techniques including rules, method and tools to develop, integrate, realize orchestration and share configurable assets (data, modules, analytics, applications, etc.) for Cyber and Information Warfare system;

(2) Provide standardization and interoperability recommendation;

(3) Functional analysis of typical scenarios covering use cases that will be implemented to support Toolbox demonstrations, such as:

- Attacks against deployed forces in operations;

[22] 'System prototype' means a model of a product or technology that can demonstrate performance in an operational environment.

[23] 'Qualification' means the entire process of demonstrating that the design of the product, component or technology meets the specified requirements, providing objective evidence by which particular requirements of a design are demonstrated to have been met.

[24] 'Certification' means the process by which a national authority certifies that the product, component or technology complies with the applicable regulations.

- Attacks of hybrid nature below the threshold of conventional warfare against critical entities and functions in whole-of-society, including defence and military.

(4) Operational concept of usage, including use of AI and efficient situation awareness tools, consistency with rules of engagement (RoE), management of counterintelligence, and trustworthiness;

(5) Algorithm prototyping, implementation and verification, including the data sets and metrics to be used to do so for the purpose of the above use cases;

(6) Development tools including algorithm insertion, integration in demonstration environment and run of demonstration to illustrate the use of the Toolbox for the two above use cases.

The proposals must substantiate synergies and complementarity with general command and control processes and functions, avoiding unnecessary duplication with projects previously awarded.

The following task may be performed as part of the activities:

- Studies regarding societal and cultural impact of disinformation and (blue & red) state-led communication campaigns.

The proposals could benefit from framework, or results coming from projects previously awarded, increasing synergies and effectiveness of targeted activities.

Functional requirements

Proposals should meet the following functional requirements:

I Information Warfare

Developing information manipulation identification, “Disinformation Tracking” use case (including modelling influence and opinion propagation, user behaviour analysis, community detection in social graphs, detect disinformation campaigns, identify disinformation, with trustworthiness score) in favour or against Information Warfare Operations in the context of Multidomain Operations.

In order to offer situational awareness and support to decision process, proposals should elaborate on:

- identified threats activities (hostile influencing avatars and groups);
- campaign with scorings levels like trust, importance (followers, retweets), severity and friendly targets;
- used artifacts (pictures, texts, video) that can be identified as fake/reused items;
- when possible, additional information providing hints on physical sources of information operations attacks (e.g., images metadata or details, IP addresses, etc.)
- identification of "archetypes or patterns” of fakes to increase interception capabilities, both in a ‘humanity’ and through a ‘technology’ approach;
- Interactions with other sources of information, such as open source and human intelligence (OSINT, HUMINT), that could be related with operations in cyber domain and used for optimisation and synchronisation.

II Emerging Technologies

Proposals should identify emerging technologies that can be applied on automatic image/video/text entities extraction/indexing/classification/fusion and be subject to further research and development, such as:

- Active Learning (to allow operators to make their own classifiers with their own data)
- Case-based Reasoning (CBR) or other metacognition enablers to create different levels of knowledge abstraction
- Transfer/Frugal Learning (to be able to learn from small amounts of data)
- Hard and Soft Fusion (to fuse data and information from different sensors and sources, including semantic information)
- Explainable AI (to ensure that all AI algorithms are transparent and that the operators can have a look into AI decisions for understanding if needed)
- High precision 3D modelling
- Method and toolkit for assessing performances and security aspects (ethics guidelines, elimination of biases, compliance with GDPR, system protection etc.).
- Situational awareness and corresponding decision aids (to track incidents, link them into a campaign, and issue recommendations and alerts).

III Standards and interoperability

To develop and promote assets in the Toolbox, proposals should comply requirements such as technology standards (API, encapsulation), data exchange and interoperability standards, intellectual property protection, traceability, and authentication.

Proposals should:

- Define a set of standards' proposals that allows multi-national collaboration, sharing of data and sharing of assets like for example machine-learning models for military use.
- Define guidance for AI-based defence projects development.
- Contribute to a proposal to standards integration of new technologies such as AI in Cyber and Information Warfare system and more broadly for defence application.
- Compile existing standards and contribute to a proposal to standards for trustworthy AI in defence.
- Ensure that the project leverages technological capabilities while at the same time addressing the ethical issues involved.
- Explore harmonisation of existing tactics, technologies, and policies.

Expected impact

The outcome is expected to contribute to:

- Optimizing the development and integration of analytics in Cyber and Information Warfare systems with the possibility to decrease cost;
- Increasing the European technological sovereignty in the field of Cyber and Information Warfare applications based on AI;
- Increasing of the overall Cyber and Information Warfare system performance as new technologies will give better results in terms of total defence effectiveness;
- Gain on costs, availability and interoperability by optimizing the development and integration of analytics in Cyber and Information Warfare systems and capitalizing at European level Cyber and Information Warfare assets.

EDF-2022-DA-CYBER-CSIR: Cybersecurity and systems for improved resilience

Objectives

General objective

Kinetic and digital military operations increasingly rely on computers and networked communications for information gathering, intelligence, coordination and weapon control. At the same time as the dependencies on digital technologies rapidly grows, so does the potential threats and vulnerabilities. The global community, military, and battlefield may be affected by increasing threats. Furthermore, the Internet of Things (IoT) has become widely integrated into a variety of sectors and industries, offering "readymade" solutions for surveillance, monitoring, healthcare, and military platforms. Examples for IoT devices are drones, software defined radios, sensors (cameras, humidity, temperature), TV devices, cars/vehicles). Many IoT solutions are designed primarily for functionality, without being properly secured. As a result, attacks on IoT environments have gained momentum due to the increased attack surface. Therefore, the need for cybersecurity services, including ensuring an appropriate level of control and prevention (e.g., over data, communications, systems), must be addressed.

Specific objective

Currently, many cybersecurity solutions are being used or under development or research. However, cyber threats continue to evolve affecting the systems and services on which today's community relies.

A test environment is imperative to determine how to enhance the security of a system, product, or component, through the generation of effective tests for analysing the system in question, its threat response capability, resulting in forensic dissemination, procedures, and proposals of improved architectures.

Most legacy specialized military systems are not directly vulnerable to cyber-attacks and malware employed in the open Internet, yet a growing use of ICT/IoT Commercial Off The Shelf (COTS) components and increasing connectivity may increment the likelihood of targeted attacks using the methods, if not the tools, used in cyber-attacks on the open Internet.

The increasing use of the cyber domain will require defence forces to operate in unexpected scenarios and consequently systems to function outside the environments they were designed for.

It is thus essential to understand the extent of the threat, develop infrastructure to continuously assess security against an evolving threat landscape, build resilience by guaranteeing mission assurance even with a partial compromise also using trustworthy hardware, software applications, communication protocols and trustworthy operating system.

Scope and types of activities

Scope

Proposals are expected to prepare, design and/or demonstrate a Cyber Physical Test lab with hardware and software tools supporting expertise focusing on generation of effective tests for common and relevant Cyber Physical systems, products and components with realistic data from a relevant use case.

It must provide capabilities for cybersecurity analysis of the actual and planned system architecture, including a demonstrated threat analysis of a selected system or component. Based on this analysis, the architecture can be updated in order to increase the security of the system to an appropriate level.

Integrated tools for automated cost-efficient cyber validation tests based on requirements indicated by international standards may be included. The tools should be able to emulate system being tested, store detailed configurations, conduct automated testing and validation of military architecture, store the results and be able to repeat testing periodically in a cost-effective manner, considering system reconfiguration and extension during the lifecycle and the updated threat landscape.

The proposals are expected to contribute to enhancing cybersecurity in the Member States and Norway critical digital information infrastructure- solutions and services within security, encryption and communication systems, from strategic to tactical level.

Types of activities

The following table lists the types of activities which are eligible, and whether they are mandatory or optional *(see Article 10(3) EDF Regulation)*:

Types of activities (art 10(3) EDF Regulation)		**Eligible?**
(a)	Activities that aim to create, underpin and improve knowledge, products and technologies, including disruptive technologies, which can achieve significant effects in the area of defence (**generating knowledge**)	No
(b)	Activities that aim to increase interoperability and resilience, including secured production and exchange of data, to master critical defence technologies, to strengthen the security of supply or to enable the effective exploitation of results for defence products and technologies (**integrating knowledge**)	Yes (optional)
(c)	**Studies**, such as feasibility studies to explore the feasibility of new or upgraded products, technologies, processes, services and solutions	Yes (mandatory)
(d)	**Design** of a defence product, tangible or intangible component or technology as well as the definition of the technical specifications on which such a design has been developed, including any partial test for risk reduction in an industrial or representative environment	Yes (mandatory)

(e)	**System prototyping**[25] of a defence product, tangible or intangible component or technology	Yes (optional)
(f)	**Testing** of a defence product, tangible or intangible component or technology	Yes (optional)
(g)	**Qualification**[26] of a defence product, tangible or intangible component or technology	Yes (optional)
(h)	**Certification**[27] of a defence product, tangible or intangible component or technology	Yes (optional)
(i)	Development of technologies or assets **increasing efficiency** across the life cycle of defence products and technologies	Yes (optional)

The proposals must include study and design activities. The proposal may include other eligible downstream activities.

The following tasks should be performed as part of the required activities:

- Phase 1: Perform requirements analysis, development of concepts and procedures, definition of architecture and design a Cyber Physical Test lab with expert hardware and software test tools and integrated tools for validation.
- Phase 2: Implementation and demonstration of a Cyber Physical Test lab with HW[28] & SW[29] test tools that focus on generation of effective test, forensic dissemination, procedures and architecture to ensure cybersecurity for common and relevant Cyber Physical systems, products and components, including addressing Digital Twin applications in the military supply chain over the lifecycle.

The final product/ system must be able to analyse the security of a system in order to ensure:

- Data integrity
- Data control
- Data Loss Prevention
- Communications control
- Meta Data control
- Operational control of Cyber Physical components for common and relevant Cyber Physical systems, products and components
- Ability to guarantee mission-essential capabilities even with partial compromise.

[25] 'System prototype' means a model of a product or technology that can demonstrate performance in an operational environment.

[26] 'Qualification' means the entire process of demonstrating that the design of the product, component or technology meets the specified requirements, providing objective evidence by which particular requirements of a design are demonstrated to have been met.

[27] 'Certification' means the process by which a national authority certifies that the product, component or technology complies with the applicable regulations.

[28] Hardware.

[29] Software.

The final product (Cyber Physical Test Lab) must comply with existing and foreseen standards, including military standards.

Functional requirements

The proposal should support the development of the final product.

The final product (Cyber Physical Test Lab) should meet the following functional requirements:

- Provide physical access to dedicated computers for instrumentation and software development. Part of the Lab may be restricted (classified) according to specific needs deriving from the products and components being tested;
- Generate effective penetration tests to evaluate the security of a system or a component, using state-of-the art tools;
- Generate customizable network traffic for testing and evaluating systems and solutions, and their security;
- Provide specialized resources for simulating attacks with and extendable and customizable database cyber tools for network traffic, services, IoT devices and communication in a customizable with the capability to automate attacks;
- Provide solutions and support to develop and debug embedded systems;
- Perform static analysis of embedded software, in order to improve security in IoT;
- Configure Cyber Physical systems according to appropriate and robust architecture for specific and customised use by Member States and Norway;
- Address the use of Digital Twin applications in the military supply chain over the system lifecycle;
- Monitor and control the communications between cyber physical components, systems, and the external environment through a state-of-the-art software;
- Provide a library of procedures to render a component or a system safe to use under specific conditions;
- Create a database with information on the risk of using various components of a system;
- Provide recommendations on risk mitigating techniques and risk management for a system or a component of a system;
- Provide capability in order to store the configuration of systems/components to be tested, enabling efficient periodic testing and whenever possible automated setup of configuration to be tested;
- Provide capability to store results, formal description of the system being tested, performed attacks, attack propagation, effect on functionalities and services, and compute a set of KPIs specialized for different types of technology / solution being tested;
- The lab should be a centralized or federated system. Federation should be used when needed in order to ease testing and validation, within a common technical and methodological framework, of components of national interest.

Expected impact

The outcome should have a major impact on the Member States and Norway' economy and cybersecurity cooperation, through:

- Establishing state-of-the-art test facility and competences, procedures and forensic software for Cyber Critical systems.
- Enabling IoT third parties to be used in a more secure, effective and economical way both in legacy, and novel systems.
- Decreasing implementation cost and shortening implementation time for advanced cyber security systems for the cooperating Member States and associated countries.
- Enabling the use of secure third-party components in Cyber Critical systems, leading to increased flexibility and competitiveness for the cooperating Member States and associated countries.
- Contributing to the certification of systems and to the EU Cybersecurity Certification framework, including contributing to enhance "security by design" of new systems and identify threats related to the supply chain.

EDF-2022-DA-SPACE-ISR: Innovative multi-sensor space-based Earth observation capabilities towards persistent and reactive ISR

Objectives

Space-based Intelligence, Surveillance and Reconnaissance capabilities are core enablers for Defence and Security missions.

Today, several European Member States own or are developing sovereign high-end space-based optical, SAR[30] and SIGINT[31] assets and associated capabilities allowing them to understand crises and complex situations outside Europe and at its boundaries. Those assets, necessary to monitor and react effectively to different threats and events related to national and international security and safety, are currently being developed nationally with different degrees of governmental and industrial collaboration in accordance with the different national and international policies and priorities.

However, these highly performing assets allow only limited revisit over an area of interest. They do not permit either a quick and smart reaction to an event detected on-board or a very quick satellite tasking and data reception upon a decision taken on the ground. Besides, some imagery applications of high interest for defence (such as optical video, low light, infrared or hyperspectral imagery and on-board processing for faster and more efficient transmission) remain insufficiently covered.

General objective

This topic aims at developing an affordable constellation of small satellites, including its ground segments able to handle various types of sensor payloads (*e.g.,* optical video, low light, infrared, hyperspectral, RADAR, SIGINT) for Intelligence, Surveillance and Reconnaissance (ISR) applications. Such a constellation would complement high-end existing military capabilities while allowing responsive and smart tasking and data collection for near real-time tactical use.

[30] Synthetic aperture radar.

[31] Signal intelligence.

This topic may also pave the way towards a collective and concerted approach regarding a future operational European Earth observation capability for ISR applications.

Specific objective

The specific objective of this topic is to define the overall architecture of the constellation, with particular attention to miniaturization, responsiveness, affordability, and complementarity with on-going EU and national projects, and to develop the associated components (sensors, platforms, ground segments and other key sub-systems), providing global and reactive coverage to address Member States, associated countries and EU needs in terms of innovative ISR capabilities and near real time intelligence.

One of the challenges is to achieve high performance payloads compatible with small satellites, in order to procure an affordable constellation that can federate European Member States and Norway around a shared capability. In this context, industry will have to propose a development that leads to an affordable solution in terms of non-recurring and recurring costs. Indeed, high revisit capability and need for variety of sensors inherently requires deploying a constellation(s) of assets: the proposed development must therefore particularly look into miniaturised, mutual and/or standard components for the satellite platforms and payloads in order to reduce the costs, and into solutions for high data rate transmission and processing.

The topic will also have to address the challenge of ensuring that the proposed solution can be adapted to various forms of cooperation (at transnational and/or multi-agency level) to build, following the EDF project, a full-fledge multi-user and multi-sensor constellation, be its components and/or the full constellation jointly or nationally procured.

Scope and types of activities

Scope

Project proposals must address the development of a European space-based Earth observation multi-sensor constellation of small satellites for ISR applications. It must include the definition of the concept of operations (CONOPS) for such capability, its overall architecture including system level activities (*e.g.,* choice of orbits, inter-satellite links (ISL), data relay satellites, ground stations, raw data management and processing and ISR post-processing analysis) and the definition of each component of the end-to-end system, composed of the satellite platform, the ISR payloads and the ground segment(s).

Project proposals must consider various options for each component of the system based on existing solutions, adapted solutions and/or new developments. Different development stages can be considered for the project, depending on the current maturity level for each component or ISR payload. Synergies with industrial technology roadmaps and with national, multinational and EU programmes, studies and projects (*e.g.,* EDIDP, EDA, EU space programme/secure connectivity) are also encouraged.

Project proposals must not duplicate the work requested in 2020 in the call topic EDIDP-MSC-MFC-2020 *Multifunctional capabilities, including space based surveillance* *and tracking, able to enhance the maritime awareness (discover, locate, identify, classify and counteract the threats)*[32].

Types of activities

The following table lists the types of activities which are eligible, and whether they are mandatory or optional *(see Article 10(3) EDF Regulation)*:

Types of activities (art 10(3) EDF Regulation)		**Eligible?**
(a)	Activities that aim to create, underpin and improve knowledge, products and technologies, including disruptive technologies, which can achieve significant effects in the area of defence (**generating knowledge**)	No
(b)	Activities that aim to increase interoperability and resilience, including secured production and exchange of data, to master critical defence technologies, to strengthen the security of supply or to enable the effective exploitation of results for defence products and technologies (**integrating knowledge**)	Yes (optional)
(c)	**Studies**, such as feasibility studies to explore the feasibility of new or upgraded products, technologies, processes, services and solutions	Yes (mandatory)
(d)	**Design** of a defence product, tangible or intangible component or technology as well as the definition of the technical specifications on which such a design has been developed, including any partial test for risk reduction in an industrial or representative environment	Yes (mandatory)
(e)	**System prototyping**[33] of a defence product, tangible or intangible component or technology	Yes (optional)
(f)	**Testing** of a defence product, tangible or intangible component or technology	Yes (optional)
(g)	**Qualification**[34] of a defence product, tangible or intangible component or technology	Yes (optional)
(h)	**Certification**[35] of a defence product, tangible or intangible component or technology	Yes (optional)
(i)	Development of technologies or assets **increasing efficiency** across the life cycle of defence products and technologies	Yes (optional)

The following tasks must be performed as part of the mandatory activities of the project:

– Studies

[32] https://ec.europa.eu/info/funding-tenders/opportunities/portal/screen/opportunities/topic-details/edidp-msc-mfc-2020.

[33] ‘System prototype’ means a model of a product or technology that can demonstrate performance in an operational environment.

[34] ‘Qualification’ means the entire process of demonstrating that the design of the product, component or technology meets the specified requirements, providing objective evidence by which particular requirements of a design are demonstrated to have been met.

[35] ‘Certification’ means the process by which a national authority certifies that the product, component or technology complies with the applicable regulations.

  - the development of the CONOPS, possibly considering existing space ISR capabilities in order to develop a robust and secure system. The CONOPS must:
    - include the description of how the user interacts with the ISR constellation, and how relevant parts of the tasking, collection, processing, exploitation, and dissemination (TCPED) process are done, including in terms of multi-users resource sharing and automation of the mission planning/image chain to reduce the operation activities and costs and improve timeliness of information;
    - be developed considering current and expected threats, in order to steer the feasibility analysis and the design phase in terms of integrity, confidentiality and availability requirements at both space and ground segment levels;
    - investigate the use of existing private and governmental assets to define and tune its development;
    - consider as an objective to reduce the manpower needed to operate the system from mission planning to data processing, taking also into account the limited resources available on-board small satellites;
    - where possible, take into consideration as a starting point, for the end-user consultations, the needs and requirements already commonly agreed by the Member States and Norway.
  - the consolidation of the mission requirements;
- Design
  - the design and definition of the end-to-end capability (constellation architecture, type of satellites and sensors, associated ground segments, including operations support tools, interfaces) meeting mission requirements at least up to the Preliminary Design Review (PDR); as part of this task, the following elements must be considered:
    - the type of constellation and orbits (*e.g.*, sun-synchronous, elliptical, inclined orbits) to maximise revisit over the areas of interest as defined in the CONOPS, while allowing for non-predictable patterns and/or observation of a given scene under a variety of conditions;
    - the type of sensors on each satellite and on different satellites to optimize collection and processing of data with respect to the type of objects of interest (ability to detect, classify, identify) and operational/environmental conditions (day/night, clouds, presence of threats…);
    - the ability to re-task for gathering additional information, for example by tipping and cueing on other satellites of the constellation and/or interfacing with external systems;
    - the technical and operational architecture, including procedures and autonomy;

- the design and definition of the associated components (platform, sensors and ground segments) and key enabling technologies;

  - innovative ISR payloads (*e.g.,* optical video, low light, infrared, hyperspectral, SAR, SIGINT, electro-magnetic spectrum monitoring) and associated mutualised and/or standardized platforms compatible with a small satellite format while achieving required performances;

  - flexible, scalable and modular processing capacity (at space and ground segments level) allowing the implementation and testing of a variety of functionalities such as, for example, cloud detection and re-tasking, change detection, target detection, classification and recognition, resolution enhancement techniques, data compression and/or selection of area of interest in order to reduce required downlink bandwidth;

  - ways to speed up satellite tasking, data delivery and information production (*e.g.,* on board processing, autonomy, inter satellite link (ISL), use of space-based data relay infrastructure, ground stations and gateways and developing innovative communication systems);

  - scalable and modular architectures for the space and ground segments, defining mutual/standardized interfaces and building blocks and thus allowing for easy scalability of the system as well as modular exchange of components for adapting to different missions and operational needs;

  - ground stations and dissemination network design and alternatives (*e.g.,* higher frequency band) to improve the data rate and compensate the low on-board transmitting power and automatic allocation of contact opportunities;

  - ISR data processing solutions (*e.g.,* making use of AI[36]-based and/or high-performance computing technologies) in order to obtain a better situational awareness, considering the reuse and complementarity of functionalities and infrastructures available in the EU and developing dedicated interoperability layers to allow a secure and effective exchange of data among the EU Member States and associated countries;

  - definition of generic import/export functions and formats in view of possible interface with external systems such as governmental and commercial systems and database;

  - encryption means both for the downlink and the uplink, in order to provide secure communication links for military, governmental or any other application that requires confidentiality.

The following tasks may be performed as part of the optional activities of the project:

- Prototype

[36] Artificial intelligence

  - the development of a prototype for selected payloads and/or subsystems;

- Testing and qualification

  - testing (test campaign) and qualification (up to qualification review) of selected payloads and/or subsystems.

Functional requirements

The capability to be developed should meet the following functional requirements:

- **high revisit**: develop a scalable solution allowing to accommodate a growing number of satellites (same or different payloads) within the constellation, ultimately to reach, for some use cases, intra-hour revisit;
- **affordable very high spatial resolution**: achieve resolution below 0.5 m with small satellites for optical visible video/still imagery and SAR (*e.g.,* low altitude orbit, on-board processing);
- **operational timeliness improvement**: develop the capability to dynamically (re)task a satellite (*e.g.,* within a few minutes); ability to perform automatic tipping and cueing; reduce downlink latency and enhance data downlink throughput; for some use cases, reduce time between tasking of the constellation and delivery of the relevant information to the end-user (*e.g.,* tactical use);
- **highly digital architecture allowing advanced and flexible on-board processing**: enable autonomous extraction of actionable information from the captured imagery and data, and automatic preparation of complementary tasking of the constellation(*e.g.* autonomous decision to lock image over a defined object or area of interest pin-pointing), even with different acquisition modes (*e.g.* video) for target detection and analysis (classification, recognition, identification) depending on task/mission, including SIGINT;
- **space-to-ground efficiency**: allow both high data rate downlink and optimisation of downlink efficiency, where relevant making use of on-board processing capabilities;
- **new space imagery and SIGINT applications for Defence and Security**: develop new sensors, processes and processing compatible with a small satellite and allowing to provide new type of products of interest for Defence and Security;
- **big data analysis**: to develop a system that could support Big Data management to achieve high-speed analysis (including fusion) and streaming of multi-sensor data for ISR purposes;
- **interoperability**: develop a system that is inter-operable with external systems (*e.g.,* with interfaces allowing information exchanges across participating Member States and associated countries and with the EU);
- **security requirements**: develop a system that takes into account the necessary needs for integrity, confidentiality and availability (this should include affordable crypto for up- and down-links) and the multi-user dimension of the constellation (while anticipating possible future access by other institutional users for civilian missions (*e.g.,* security or emergency).

Expected impact

Such new ISR capability will have a very high impact over the tactical means of the European stakeholders before and during a crisis, in term of:

- reactivity (rapid availability of information after request);
- added value of the information collected (nature, resolution and complementarity with other ISR sources).

The nature of the solution (constellation of small satellites allowing sharing of resources between EU Members States, Norway and other users) will also allow shared or joint procurement and in-service support while preserving a sufficient level of sovereignty.

EDF-2022-DA-SPACE-SBMEW: Space-based missile early warning

Objectives

General objective

Taking into full consideration the ongoing EU, Member States and Norway funded activities in this domain, the topic general objective is to contribute to the further development of a European space-based early warning capability against various types of missile threats: ballistic, hypersonic and anti-satellites (ASAT). This topic will focus on the one hand, on the consolidation of the overall system architecture and on the other hand, on the development of the critical technologies needed for such capability.

Specific objective

The specific challenges of the topic reside in the following considerations:

- recent developments and tests of ballistic missiles, hypersonic gliders and ASAT missiles have recalled the eminent and rising threat to the European people arising from those capabilities;
- there are currently neither sufficient European sensor capabilities for detection and tracking of such threats nor European capabilities available for their interception;
- until today, Europe is dependent on third-party systems for space-based early warning;
- European capabilities for ballistic missile defence (BMD) and against ASAT threats – e.g., sensor capabilities like space-based early warning and the corresponding distribution of object tracking information – are addressed in capability plans of several EU Member States and associated countries, but only partially developed and not yet operational;
- sovereignty and safety are essential for the EU as well as the capability to act, based on its own intelligence, and the ability to defend, based on its own decisions;
- the detection and interception of ballistic and hypersonic threats are complex and costly and would benefit from a cooperative approach at EU level;
- an integrated and inclusive approach to study and develop solutions in a collaborative and coordinated way using the expertise and capacities available in the EU (both at industry and government level), including dedicated national

spending, will contribute to a better and sustainable closing of the capability gap in this field.

Scope and types of activities

Scope

Project proposals must address activities needed to further develop a fully European missile early warning and tracking capability that would lead to an autonomy in the field of threat assessment and theatre defence and the ability to provide a system that is coherent, complementary and interoperable with other systems, including non-EU ones (*e.g.,* NATO systems).

More precisely, project proposals must address:

- the implementation study of a feasible space-based missile early warning (SBMEW) system and its concept of operations (CONOPS), taking into account existing development plans;
- the identification, analysis and mitigation of the critical technical and technological risks associated with the development in the EU of a SBMEW capability, taking into account the status of existing assets within European industry that can contribute to such capability.

Types of activities

The following table lists the types of activities which are eligible, and whether they are mandatory or optional *(see Article 10(3) EDF Regulation)*:

Types of activities (art 10(3) EDF Regulation)		**Eligible?**
(a)	Activities that aim to create, underpin and improve knowledge, products and technologies*,* including disruptive technologies, which can achieve significant effects in the area of defence (**generating knowledge**)	No
(b)	Activities that aim to increase interoperability and resilience, including secured production and exchange of data, to master critical defence technologies, to strengthen the security of supply or to enable the effective exploitation of results for defence products and technologies (**integrating knowledge**)	Yes (optional)
(c)	**Studies**, such as feasibility studies to explore the feasibility of new or upgraded products, technologies, processes, services and solutions	Yes (mandatory)
(d)	**Design** of a defence product, tangible or intangible component or technology as well as the definition of the technical specifications on which such a design has been developed, including any partial test for risk reduction in an industrial or representative environment	Yes (mandatory)
(e)	**System prototyping**[37] of a defence product, tangible or intangible component or technology	Yes (optional)
(f)	**Testing** of a defence product, tangible or intangible component or technology	Yes (optional)

[37] 'System prototype' means a model of a product or technology that can demonstrate performance in an operational environment.

(g)	**Qualification**[38] of a defence product, tangible or intangible component or technology	Yes (optional)
(h)	**Certification**[39] of a defence product, tangible or intangible component or technology	Yes (optional)
(i)	Development of technologies or assets **increasing efficiency** across the life cycle of defence products and technologies	Yes (optional)

The following tasks must be performed as part of the mandatory activities of the project:

- Studies:
  - consolidation of the SBMEW mission, system requirements and architecture as a basis for an implementation plan for all intended objectives of the system;
  - maturation of the SBMEW system CONOPS (if possible, supported by simulations), especially addressing the mission objectives, the strategies, tactics, policies and constraints affecting the system operation, the involved organisations, activities and interactions among operators, users from Member States and Norway, and their respective roles and responsibilities;
  - as an optional task: assessment, via models and simulation, of the added value of new imaging technologies (*e.g.,* hyperspectral) for identification of threats;
- Design:
  - definition, development and exploitation of SBMEW system simulations addressing all SBMEW missions, allowing assessment of real time and non-real time performances of the system and interoperability with external systems, including C2[40] (e.g., NATO, EU and national C2, radars, BMD and SSA[41] systems);
  - maturation and de-risking/developments of SBMEW critical subsystems and technologies (especially the detectors, the pointing mechanisms, the cooling mechanisms, the on-board computing, the sun protection and the secure satellites communication and control system), including tests of demonstrators to achieve a level of technological readiness allowing the launch of the real capability in space by end of the decade;
  - update of programmatic elements (e.g., costs, planning, risks, cooperation scheme) for the development of a European SBMEW capability.

[38] 'Qualification' means the entire process of demonstrating that the design of the product, component or technology meets the specified requirements, providing objective evidence by which particular requirements of a design are demonstrated to have been met.

[39] 'Certification' means the process by which a national authority certifies that the product, component or technology complies with the applicable regulations.

[40] Command and control.

[41] Space situational awareness.

Functional requirements

The proposed development should fulfil the following requirements:

- the architecture of the SBMEW system should be composed of:
  - a space segment;
  - a ground segment (mission and control);
  - a user segment
- the CONOPS should address:
  - operations planning, real time operations and deferred time operations;
  - intelligence missions;
  - joint operations with non-space sensor systems for launches observation and space surveillance;
  - joint missions with external sensors and effectors for early warning and missile defence;
- the SBMEW simulations should include for all missions:
  - an integrated representation of the threat;
  - an integrated representation of the environment, including the presence of clouds and sun impact;
  - an integrated representation of the space sensors and platforms including their tasking;
  - on-board and on-ground image and data processing algorithms which should:
    - be able to represent the detection of the threats by the space sensors considered;
    - be able to measure and estimate the trajectory of all detected launches (including related accuracy/uncertainty and launch departure point and predicted impact points);
    - allow to contribute to aggressor identification and to recognise the detected ballistic missiles and launchers within a catalogue of known objects or to identify them as unknown;
  - a demonstration, against all threats, of an end-to-end analysis of SBMEW real-time and non-real-time performances with synthetic data for consolidation of the mission and observation requirements;
  - a demonstration of interoperability with external systems (*e.g.,* NATO, EU and national C2, radars, BMD and SSA systems);
  - an interface with external data providers (*e.g.,* military SSA catalogues);

  - demonstration of agility of the system to cope with operational mission change/ evolution;
- the SBMEW risk mitigation activities of the critical subsystems and technologies should include:
  - study and stepwise breadboard if required, to achieve sufficient technological readiness level;
  - detectors;
  - cooling mechanisms;
  - pointing mechanisms;
  - sun protection;
  - on-board computing;
  - Satellite reliable secure command/control and Early Warning Communications

Expected impact

Implementation of a European collaboration on this topic will:

- allow sharing of resources and building a common operational view on ballistic, hypersonic and ASAT missile threat assessment;
- augment dramatically EU political power and international credibility towards superpowers for control of international regulations, control of international treaties, intelligence on missile technology development in specific countries and if necessary operational theatre defence capability.

Beside the establishment of a European sovereignty, it can furthermore provide a significant and valuable in-kind contribution to NATO BMD.

EDF-2022-DA-MATCOMP-SMT: Smart and multifunctional textiles

Objectives

General objective

Soldier equipment needs to allow for activities that are often physically demanding, while bringing protection, situational awareness and preserving capacity to act, endurance, and mobility. The garment is an integral part of that equipment and must meet this challenge. Smart and multifunctional textiles are a new generation of materials and systems with multifunctional properties which, given their ability of being integrated into uniforms, have drawn the attention of the defence community. Smart textiles are defined as textiles able to interact with their surroundings: they respond and adapt to a given stimulus. Functional textiles provide an additional and specific function through their composition, their construction and/or their finish. Typically, these functions encompass enhanced mechanical resistance, water and/or dirt repellence, fire retardancy, antibacterial properties, protection against ultraviolet radiation, pest or chemicals, thermal isolation, etc.

Smart and multi-functional textiles pave the way to multiple possibilities for developing high-tech garments responding to multiple needs in an elegant solution. These materials enable to integrate different components and devices, in a comfortable and ergonomic way, providing a wide range of functionalities that can improve the safety, performance and wellbeing of the soldiers. Moreover, those textiles also offer new integration opportunities with platforms and systems.

Specific objective

An example for a challenge linked to the physically demanding work in harsh environmental conditions is the management of heat stress. Non-compensable heat stress can lead to physical and cognitive performance losses as well as life-threatening heat-related illnesses. Root cause are conditions specific to the military service: Soldiering is hard physical work, often in protective clothing due to complex threats (e.g., ballistic body armour, Chemical Biological, Radiological and Nuclear (CBRN) protective gear) whose insulating properties impede or even prevent the dissipation of work-induced metabolic heat build-up. Heat dissipation is especially impaired in hot climate zones.

Another key challenge in the defence context is to ensure that soldiers will have the best chances of survival through fast and live saving medical treatment when seriously wounded in a military conflict or battle situation. In case of a large number of severe injured soldiers, it is necessary to have a fast and precise assessment of the critical status of the victims to calculate the number and treatment priority by triage through an emergency physician. If vital signs like pulse rate, blood pressure, oxygenation and other vital information like blood loss, trauma and electrocardiogram can be determined fast and transmitted from the incident by the use of wearable sensor systems wireless to the emergency physician who performs the triage and first medical treatment, the effectiveness of care and chance for survival can be improved.

The soldier of the future will need technological solutions to sensor and monitor information coming from both its surrounding (such as threats) and its physiological state (parameters associated with the stress experienced by the soldier and its health condition, etc.). Another important aspect is the ability of knowing their location with a high level of precision, as well as being able to receive and provide information related to their present situation. Furthermore, these additional functionalities will also mean more information exchange between the soldier and its equipment. Innovative human-machine interface (HMI) directly integrated into the textile will therefore enable to control the implemented functionalities or to get feedback from them while preserving or even enhancing mobility and ergonomic aspects. Furthermore, smart textiles will have to ensure the safe operation of wearable electronics and enable safe communication, considering the importance of protecting electronic equipment, data and soldiers against electromagnetic radiation.

Smart and multi-functional textiles enable to integrate different components and devices in uniforms and soldier systems and to widen their range of functionalities. To respond to challenges such as the ones listed above, functionalities can include monitoring of the environment and of the soldier's physiological state, localization, communication, energy management, protective functionalities (e.g., protection against the environment, signature reduction, including thermal radiation, fire protection, electromagnetic radiation protection and neutralization of dangerous chemicals).

Scope and types of activities

Scope

Though single technology demonstrators have been developed in the EU, further efforts are necessary on the way to an integration of smart and multi-functional textiles as one module of performant soldier systems, which would require, amongst other, standardized connectors.

This topic targets the integration of smart and multi-functional textiles and other components into a modular and ergonomic set of equipment adapted to defence applications. Standardized interfaces and protocols are a key aspect to enable modular and flexible integration of components providing different functionalities.

The scope of the topic encompasses necessary adaption of materials and technologies, development of a system concept, design of soldier equipment adapted to different use-cases, the development of a prototype and testing.

All innovative solutions should preserve soldier mobility, comfort and ergonomic aspects should therefore be considered with great care. Besides, all weight reduction opportunities, washability and maintenance requirements compliance will play a key role in making these solutions of interest. In order to minimize environmental impact, eco-design and life cycle analysis tools should be used as much as possible.

Solutions should be in line with ongoing and past projects in the field of smart textiles (e.g., EDA project STILE) and soldier equipment to avoid unnecessary duplication. Proposals should give a particular focus to potential inclusion of technologies developed in R&D activities targeting civil applications. Solutions should take into account interoperability aspects, e.g., connector standards developed in relevant international frameworks.

Types of activities

The following table lists the types of activities which are eligible, and whether they are mandatory or optional *(see Article 10(3) EDF Regulation)*:

Types of activities (art 10(3) EDF Regulation)		**Eligible?**
(a)	Activities that aim to create, underpin and improve knowledge, products and technologies, including disruptive technologies, which can achieve significant effects in the area of defence (**generating knowledge**)	No
(b)	Activities that aim to increase interoperability and resilience, including secured production and exchange of data, to master critical defence technologies, to strengthen the security of supply or to enable the effective exploitation of results for defence products and technologies (**integrating knowledge**)	Yes (optional)
(c)	**Studies**, such as feasibility studies to explore the feasibility of new or upgraded products, technologies, processes, services and solutions	Yes (mandatory)
(d)	**Design** of a defence product, tangible or intangible component or technology as well as the definition of the technical specifications on which such a design has been developed, including any partial test for risk reduction in an industrial or representative environment	Yes (mandatory)
(e)	**System prototyping**[42] of a defence product, tangible or intangible component or technology	Yes (mandatory)
(f)	**Testing** of a defence product, tangible or intangible component or technology	Yes (mandatory)

[42] 'System prototype' means a model of a product or technology that can demonstrate performance in an operational environment.

(g)	**Qualification**[43] of a defence product, tangible or intangible component or technology	Yes (optional)
(h)	**Certification**[44] of a defence product, tangible or intangible component or technology	Yes (optional)
(i)	Development of technologies or assets **increasing efficiency** across the life cycle of defence products and technologies	Yes (optional)

Among other tasks that the applicants deem necessary, the following tasks should be performed as part of the mandatory activity 'Study':

- eco-design study to assess compliance with EU current legislations and foreseeable coming regulatory rules.

Among other tasks that the applicants deem necessary, the following tasks must be performed as part of the mandatory activity 'Testing':

- the testing in a controlled environment;
- the testing in an uncontrolled environment;
- evaluation of the impact of the added functionalities on signature reduction of the prototype
- evaluation of the impact of the added functionalities on mechanical resistance of the smart and multifunctional textile solution

Functional requirements

The solution to be developed should meet the following general functional requirements:

- modularity of the equipment to adapt it to mission's requirements
- integrated system's approach, ensuring the integration of the sensors and interfaces in the soldier's system
- overall complementarity and interplay of functions
- practical, comfortable and ergonomic solution for the soldier, in particular with limited weight
- solutions should ensure that added functionalities remain compatible with:
  - signature reduction function
  - ballistic and protective functions
  - textile mechanical properties
  - washability or other maintenance and durability

[43] 'Qualification' means the entire process of demonstrating that the design of the product, component or technology meets the specified requirements, providing objective evidence by which particular requirements of a design are demonstrated to have been met.

[44] 'Certification' means the process by which a national authority certifies that the product, component or technology complies with the applicable regulations.

  - ease of movement and ergonomic functions

The solution to be developed should meet the specific functional requirements in the following areas of priority:

- In the field of thermoregulation:
  - active or passive regulation of body temperature in case of extreme weather conditions (hot or cold)
  - consideration of both static and dynamic missions as use cases for thermoregulation.
- In the field of monitoring of the environment and functionalities regarding the soldier's physiological state:
  - monitoring of various physiological data for dedicated use cases.
  - drug delivery and/or emergency care to act on blood loss and other traumas, using data collected through monitoring
  - acquire localization data
  - protection of medical collected data all along the process to comply with confidentiality
  - compliance of processing and utilization of medical data with ethical rules
  - protection of the data collected for environment and equipment monitoring
  - data formats corresponding to relevant standards and connection with relevant interfaces.
- In the field of Energy management:
  - integration of energy conversion and distribution through textiles, with consideration of soldier architecture in particular to replace heavy and bulky cables and connectors

Moreover, the solution to be developed should additionally meet functional requirements in at least one of the following areas (Applicants must clearly indicate in their proposal, which of these functional areas they chose to address):

- In the field of protection from environmental hazard:
  - resistance to mechanical damage
  - fire resistance of external layers,
  - protection against mosquitos and other parasites
  - alternative solutions to textile treatments that are incompatible with current and coming regulations (e.g., alternatives to Per- and polyfluoroalkyl substances (PFAS) treatments)
- In the field of Energy management:

  - innovative capabilities of energy storage, e.g., novel high-performance textile-based batteries and supercapacitors
  - innovative solution for energy harvesting, e.g., by textiles and fibrous chargers.
  - compatibility of the energy management system with textile characteristics (flexibility, elasticity)

- In the field of electromagnetic protection and electromagnetic interference protection:
  - safe and reliable operation of wearable electronics and safe communication between the components in environments with broad-spectrum electromagnetic radiation, e.g., in the case of high power electromagnetic (HPEM) or other-Directed Energy Weapon (DEW) attacks
  - protection of the soldier against electromagnetic radiation of high intensity
- In the field of human-machine interfaces:
  - full integration of innovative HMI solutions in soldier clothes
  - ease of access to information, presentation of information adapted to the operational situation
  - adapted interaction functions with the equipment, e.g., new ergonomic interaction functions, adapted actuators, touchscreens.
  - communication functions
- In the field of monitoring of the protective equipment:
  - monitoring of the functions of the smart multifunctional textile
  - monitoring of the protective capabilities of the uniform for analysis and recording
  - provide location data on the equipment

Expected impact

- Enhancement of soldiers' capacity to perform their demanding tasks during military operations
- Increased safety and well-being for the soldier
- Increased interoperability of smart and multifunctional components for EU Members states and Norway defence forces
- Improvement of industrial and technical know-how on smart and multifunctional textiles in the EU Member States and Norway
- The capacity of technology and industry actors in the EU Member States and Norway to develop soldier equipment that is compliant with EU specific regulatory and ethical requirements

EDF-2022-DA-AIR-AEW: Airborne electronic warfare

Objectives

The proliferation of advanced long-range Integrated Air Defence Systems (IADS), incorporating threats that can operate across different frequency bands and attack aircraft at ranges up to 400 km, could create Anti Access/Area Denial (A2/AD) areas. In such A2/AD areas, which could equally affect EU Member States' and associated countries' airspace, air operations including projection of forces by air would not be possible in case of emergence of a crisis.

General objective

As European forces increasingly face sophisticated long range IADS and A2/AD systems, airborne electronic attack (AEA) capabilities become essential to create safe bubbles around formations of aircraft. From the operational perspective, the AEA capability must be able to mitigate Electro Magnetic (EM) threats in the largest possible Radio Frequency (RF) spectrum used in military operations. The effects should be coordinated with stand-in, stand-off, self-protection of manned and unmanned platforms. This implies to operate in a consistent and a synergetic way all the assets of the electronic warfare (transmitter, receiver) that would be in motion and in different places.

Specific objective

The main challenge is therefore to enable any platform involved in AEA missions to adapt to the latest in electronic warfare (EW) requirements, which include (soft) suppression of enemy air defences, escort role, electronic attack, self-protected/time-critical strike support, and continuous capability enhancement.

Currently the EU Member States and Norway capabilities in countering these threats are limited and when needed, most of the required capability is provided by NATO allies. Moreover, AEA has been identified by the Council as a main CSDP military capability shortfall (High Impact Capability Goal) to be addressed in the medium term. The EU Capability Development Plan (CDP) also identifies electronic attack as one of the priority areas for development.

Against this background, the objective of this call is to carry on the development of a set of building blocks to be installed in different platforms and systems leading to reduce the operational risks related to EU Member States and Norway air force engagements within European territories as well as the force-projection in other potential areas of operations.

Scope and types of activities

Scope

The objective must be the development of complementary building blocks technologies and components addressing the electronic warfare challenges and the development and the production of a prototype as an airborne electronic attack capability demonstrator by the end of 2027, which would validate this conceptual approach, help decision-making and reduce risks for possible further investments.

In addition, a feasibility assessment is required regarding the creation of a digital environment system capable to reduce development risks, costs and length, minimizing experimental tests at the test range and carrying out system performance checks even in "flight line".

Threat identification and tracking should be addressed, as the prerequisite for effective electronic counter measure (ECM).

Proposals should also define requirements for an electronic warfare mission planning/report system in order to:

- Dimension the complexity and heterogeneity of the platforms that can be part of AEA capability.
- Identify near real-time reconfiguration capability and the mechanisms to be implemented to manage the need for adaptability during the mission.

Potential synergies and complementarity with ongoing projects at national, multinational or EU level must be given due consideration. In any case, proposals must not duplicate the work requested in the call EDIDP-ACC-AEAC-2019 *Airborne electronic attack capability*[45].

Types of activities

The following table lists the types of activities which are eligible, and whether they are mandatory or optional *(see Article 10(3) EDF Regulation)*:

Types of activities (art 10(3) EDF Regulation)		**Eligible?**
(a)	Activities that aim to create, underpin and improve knowledge, products and technologies, including disruptive technologies, which can achieve significant effects in the area of defence (**generating knowledge**)	No
(b)	Activities that aim to increase interoperability and resilience, including secured production and exchange of data, to master critical defence technologies, to strengthen the security of supply or to enable the effective exploitation of results for defence products and technologies (**integrating knowledge**)	Yes (optional)
(c)	**Studies**, such as feasibility studies to explore the feasibility of new or upgraded products, technologies, processes, services and solutions	Yes (optional)
(d)	**Design** of a defence product, tangible or intangible component or technology as well as the definition of the technical specifications on which such a design has been developed, including any partial test for risk reduction in an industrial or representative environment	Yes (mandatory)
(e)	**System prototyping**[46] of a defence product, tangible or intangible component or technology	Yes (mandatory)
(f)	**Testing** of a defence product, tangible or intangible component or technology	Yes (mandatory)
(g)	**Qualification**[47] of a defence product, tangible or intangible component or technology	Yes (optional)

[45] https://ec.europa.eu/info/funding-tenders/opportunities/portal/screen/opportunities/topic-details/edidp-acc-aeac-2019.

[46] 'System prototype' means a model of a product or technology that can demonstrate performance in an operational environment.

[47] 'Qualification' means the entire process of demonstrating that the design of the product, component or technology meets the specified requirements, providing objective evidence by which particular requirements of a design are demonstrated to have been met.

(h)	**Certification**[48] of a defence product, tangible or intangible component or technology	Yes (optional)
(i)	Development of technologies or assets **increasing efficiency** across the life cycle of defence products and technologies	Yes (optional)

The proposals must include the development of building block technologies and component demonstrators to support de-risking and decision-making during design phases.

By achieving a technological maturity, the envisioned prototype must have to positively qualify against environmental and EMI/EMC (electromagnetic interference/electromagnetic compatibility) requirements in order to perform airborne flight tests on the selected platforms according to the constraints of the project and the functional requirements.

Functional requirements

The capability to be developed should meet the following functional requirements:

- It should consist of:
    - Adjustable high power signal jammer in the largest possible but at least the S-band and X-band radio frequency spectrum used in military operations, able to break the acquisition cycle of radar installations since the search or early-warning phase of detection.
    - An enhanced on-board EWC2 for fast and networked electronic attack with the following capabilities:
        - Find, locate, and track electromagnetic threats.
        - Gather and merge information coming from different platforms.
        - Integrated Situation assessment and Data collection (real-time).
        - Exploit and share information on radar bands for AEA and ESM applications.
        - Data Link transmission for exploitation in real time should be possible.
        - Develop electronic collaborative operations in near real time through either own Data Link or platform DL.
- Ensure interoperability with a modular building block architecture that facilitates later adaptation to future combat systems as well as integration into NATO and national structures. These architectural building blocks should be:
    - Scalable by design as well as composed of modular and low SWaP-C enabling payloads with a swarming approach.
    - Adaptable to different operational roles with manned and unmanned platforms.

[48] 'Certification' means the process by which a national authority certifies that the product, component or technology complies with the applicable regulations.

    - Composed of (without being limited to):
        - AESA Antenna with GAN technology
        - Beam Forming
        - Digital Receiver
        - DRFM (Digital Radio Frequency Memory)
        - Processing Unit (Multi-Function-Unit) able to collect the data signals in output of each phase array unit
    - Capable to be autonomous in terms of power supply and cooling system.
    - Capable to be installed either internally in a platform or externally carried through a pod configuration.
- Be modular and using an open system architecture (OSA) approach as a reference to enable the building block architecture to be compatible with different platforms (manned and unmanned) of interest for the Member States and Norway, including pod mounted solutions. UAVs equipped with such a payload should be able to cooperate in a resilient network, utilising all advantages of swarming, *e.g.,* abundance and its geometrical dispersion, redundancy, detection and recognition hardiness, destruction vulnerability etc. It should minimise the impact on flight envelopes, altitude restrictions and flight time reduction on high endurance missions.
- It should be interoperable with the existing and planned Member States and Norway assets and systems in order to be used in joint operations, including ESM.
- It should use phased array technology for both receiving and transmitting purposes, able to generate instantaneous multi-beam with the aim to monitor the whole array spatial coverage. In particular, it should implement a highly efficient phased array based jamming system with powerful, efficient and wideband technology, with the possibility to operate in the radar band and capability to growth to communication band with cutting edge hardware to enhance the integration flexibility for a wide range of airborne platforms.
- It should either use synthetic digital modelling (Digital Twin) or create a digital environment system contributing to reduce the risks associated with the development of new complex systems, such as an electronic warfare (EW) suite.
- It should be adaptable to new and changing threats, with a high degree of reliability and efficiency, allowing to mask an entire fleet of aircraft from medium to long range, when performing different missions such as:
    - Stand-In jammer (SIJ): Small sizes and in swarms coordinated UAVs or ALD (decoys).
    - Escort jammer: Installed on a platform which guides or is part of an attacking A/C strike.
    - Stand-Off jammer (SOJ): Secure distance jamming with high Effective Radiated Power (ERP) and high sensitivity.

- It should implement specific training functions that should be used without affecting the operation of the system.
- It should allow for an easy management and development of electronic warfare libraries.
- It should feature a growth capability to perform specific cyber-attacks.

Additionally, the following functionalities should be considered:

- Development in near real time of EOB
- Analysis and Mission Planning and restitution (off-line)
- Distributed and coordinated approach to the mission
- Multi-platform cooperative jamming
- Multi-asset distributed tasks for IADS disruption

Expected impact

By developing a European airborne electronic attack capability, the action should contribute to:

- Allow EU Member States and Norway air forces to conduct operations in contested EM environment, with an acceptable level of operational risk, to deal with low-frequency radars and to counter new sophisticated threats.
- Identify key strategic components for this capability for EU and set the conditions for keeping them under the EU sovereignty.
- The development and competitiveness of EU and Norway industries worldwide by incorporating key EW components and systems currently leaded in the market by non-associated third-country industries.
- Minimize the design and development efforts that would need to be spent separately by EU and Norway industries, hence allowing for better market exploitation as well as the fulfilment of Member States and Norway armed forces requirements in the field of electronic attack.
- Boost the interoperability of electronic warfare systems among Member States and Norway armed forces, in the area of electronic attack.

EDF-2022-DA-GROUND-CGC: Collaborative combat for land forces

Objectives

The evolution of threats:

In the next 10 to 15 years, the evolution of threats will drastically change the management of land operations linked to other domains. Our forces will face a new conflict, including technological dissemination and porosity between different categories of opponents. Future asymmetric enemies will benefit from this dissemination, which may include advanced systems such as long-range antitank missiles as well as armoured vehicles and unmanned autonomous aerial and ground systems (UAxS). Threats will also reveal through immaterial and non-kinetic actions (information, cyber, electromagnetic), and even through hybrid warfare (mix of military and non-military activities). Space, which supports air-land operations, will also become a domain of confrontation.

The operational context:

A very harsh environment with high intensity activities will also characterize the future battlefield, including the land domain. Indeed, the land environment is recognized as hostile, very diverse on the planet scale, fast changing (so that existing maps rapidly do not apply anymore) and complex (with terrain compartments which may block vision as well as communication links), presenting various levels of structuration (from open to urban terrain, which represents a real challenge for image processing or for autonomous vehicles and robotics). It fully includes the 3rd dimension and thus the requirement for connectivity with other sensors and effectors in other domains (air, space and cyber) as well as underground infrastructures in urban areas. Depending on the geographical context connectivity with sensors and effectors of the maritime domain is also required. Furthermore, the cyber domain and the electromagnetic environment will be highly contested. Notably, the electromagnetic spectrum may be degraded with a dramatic impact on C2. However, the main scope of this call topic is related only to the land domain.

The technological context:

The overall protection of armoured vehicles keeps improving thanks to passive and active protection systems as well as additional layers of protection or new structure materials (lighter and more resistant). Future dismounted soldiers may benefit from mobility enhancement (with the use of light exoskeletons for instance), which will make them more agile. Automation may also play a key role in transforming future battlefields. Indeed, it may pave the way towards insensitive enemy lethal autonomous weapon systems and to fleets of UAV[49]s or ground robots, which would benefit from their numeric advantage to deal with traditional opponents. We can expect opponents that allow robotic attacks, unrestricted by man-in-the-loop for target engagements, forcing us to fight vehicle duels at machine speed. Moreover, long-range precision fires will keep developing, as well as electronic warfare capabilities. Finally, our forces may have to deal with classical ever-improving ammunitions as well as with CBRN[50] and cyber-attacks or directed energy weapons.

Technical challenges:

- Integrate real time data from a variety of sources;
- Evaluate and process big data in constrained time;
- Elaborate a middleware architecture for a future secure network and battle management system allowing efficient data distribution as well as collaborative services between platforms from different countries possibly using heterogeneous hardware solutions[51] also from different countries. The focus of this robust and secure network is on tactical level from brigade and lower since this is crucial for conducting land operations. In fact, multinational and national interoperability and data exchange is primarily lacking at the lowest levels (bottom-up approach to create a solution for the current capability gap). However, every nation requires joint interoperability and data exchange between all systems of systems at all levels. Moreover, the largest technical challenge can also be foreseen at the lower levels (company, platoon etc);
- Enhance interconnectivity and range of communication systems;

[49] Unmanned Aerial Vehicles.

[50] Chemical, Biological, Radiological and Nuclear.

[51] Taking into account the possible latency and limited bandwidth of the communication network to perform collaborative service orchestration.

- Enhance interoperability between platforms, at platform (legacy and new) and dismounted soldier level;
- Ensure cyber security and active defence of the networks;
- Ensure maintainability and technical relevance of software-based systems;
- Ensure interoperability over different generations of digital systems;
- Ensure the integration of different Battlefield Combat Identification systems;
- Elaborate C2-system architectures to avoid information overload, adapting information push to different user groups, whilst ensuring mutual situational awareness across the network;
- Ensure Electronic Warfare (EW) security, e.g., by enhancing the ability to quickly adapt to EW-threats by automated switching between different communication platforms, in addition to the existing frequency jumps in current radios;
- Ensure provisions for trend analysis enabled by algorithms in order to predict possible future adversaries' activities;
- Exploit space-based technologies, ensuring the full availability of space services;
- Develop data fusion functionality with possibility to use AI technology;
- Ensure compatibility and interoperability with Combat Cloud Services. A joint approach should be pursued from the beginning of the process. In fact, for some operations, with the development of EU collaborative warfare capabilities (ECOWAR) in the other subgroups (air, maritime, multi-domain), it is foreseeable that collaborative warfare will develop some joint capabilities for specific use-cases and interoperability with joint Strategic Command and Control Systems.

Scope and types of activities

Scope

The proposals must address the development of innovative multi-national collaborative land combat operational capabilities in order to optimize the use of the new or upgraded military land systems that are being developed by different European countries. The collaborative scenario will include all tactical levels (from dismounted soldier up to operation command post) ensuring information sharing between every entity on the battlefield through a robust flexible and secure communication framework. Furthermore, they may cover several collaborative functions ranging from geolocalisation and observation to manoeuvre or fire coordination.

They must include:

- Common analysis of operational scenarios (possibly warfare simulation), consistent with the participating Member States and Norway (pMS) planned and fielded tactical products and targeted platforms (vehicles, containers, soldiers, radios, etc.);
- Identification of key enabling technologies;

- Definition of a coordinated approach concerning middleware architecture frameworks for land collaborative combat;
- Analysis of applicable standards and norms as well as evolution proposals;
- Definition and realization of incremental real world key demonstrations (including preliminary prototyping within simulated environment).

Expected advantages and benefits of collaborative warfare:

- Speed up and improve the decision-making process;
- Reduce the time between threat detection / aggression and action or respond (e.g., manoeuvre, fire, close air support);
- Make critical information available at the right time to the right user (“actionable intelligence”);
- Share knowledge / understand a situation, in real time or near real time with our neighbouring units;
- Create and share a recognized ground picture (RGP) in real time (condition of NATO Federated Mission Network (FMN) spiral 2 and higher), to constantly update situational awareness and feed the Joint Common Operational Picture (JCOP) and vice versa;
- Enable friendly forces to gain the tactical initiative (which means presenting the situation and the options in an adequate way to the operator using adapted human machine interface (HMI), for instance with augmented reality, modelling or simulation);
- Enable a dynamic and reliable interoperability when using the different manned/unmanned platforms (size, weight, type, theatre crossing speed, presence of unmanned systems etc.) and therefore trigger mobility skills to define a complex combat collaboration among systems, which can capitalize information in order to interact efficiently and proficiently.

Consequently:

- Enhance the use of different land assets through the effective use of battle space management;
- Increase the situational awareness at the tactical level (brigade and lower);
- Reduce risks of friendly fires and collateral damage, mitigate other potential operational risks;
- Improve interoperability (in particular with respect to NATO standards including FMN compliancy, providing a further development for the European Defence Forces interoperability level);
- Ensure provisions for future “sensor to shooter” functionality;
- Increase agility and flexibility in C2 structure;
- Enhance tactical performance and decision making;
- Enhance the effectiveness and the efficiency of the military action.

Types of activities

The following table lists the types of activities which are eligible, and whether they are mandatory or optional *(see Article 10(3) EDF Regulation)*:

	Types of activities (art 10(3) EDF Regulation)	**Eligible?**
(a)	Activities that aim to create, underpin and improve knowledge, products and technologies, including disruptive technologies, which can achieve significant effects in the area of defence (**generating knowledge**)	No
(b)	Activities that aim to increase interoperability and resilience, including secured production and exchange of data, to master critical defence technologies, to strengthen the security of supply or to enable the effective exploitation of results for defence products and technologies (**integrating knowledge**)	Yes (optional)
(c)	**Studies**, such as feasibility studies to explore the feasibility of new or upgraded products, technologies, processes, services and solutions	Yes (mandatory)
(d)	**Design** of a defence product, tangible or intangible component or technology as well as the definition of the technical specifications on which such a design has been developed, including any partial test for risk reduction in an industrial or representative environment	Yes (mandatory)
(e)	**System prototyping**[52] of a defence product, tangible or intangible component or technology	Yes (mandatory)
(f)	**Testing** of a defence product, tangible or intangible component or technology	Yes (optional)
(g)	**Qualification**[53] of a defence product, tangible or intangible component or technology	Yes (optional)
(h)	**Certification**[54] of a defence product, tangible or intangible component or technology	Yes (optional)
(i)	Development of technologies or assets **increasing efficiency** across the life cycle of defence products and technologies	Yes (optional)

Functional requirements

Functional requirements range from basic information sharing to combination of information through data fusion and finally allowing non-aggressive common action.

Information sharing in order to build collective capabilities (and extend national resources while keeping full control on them):

– Map sharing: to benefit from a common and possibly extended digitized representation of the ground (with the same geographic characteristics: same

[52] 'System prototype' means a model of a product or technology that can demonstrate performance in an operational environment.

[53] 'Qualification' means the entire process of demonstrating that the design of the product, component or technology meets the specified requirements, providing objective evidence by which particular requirements of a design are demonstrated to have been met.

[54] 'Certification' means the process by which a national authority certifies that the product, component or technology complies with the applicable regulations.

typology, same grid references, etc.) seems to be a necessity for data exploitation and will facilitate a common understanding of tactical situations

  - In 2 dimensions;
  - In 2.5 dimensions;
  - In 3 dimensions.

- Collaborative blue force tracking: geolocalisation can extend to multiple friendly platforms with aggregations to present the localization of units of different sizes;
- Sharing information related to the target and disseminate the battle damage assessment;
- Collaborative observation / intelligence, surveillance and reconnaissance (ISR) (sharing of e.g., pictures, videos, plots) at the tactical level (brigade and lower);
- Sharing enemy observations, including detection, recognition, identification, location and tracking;
- Mobility information (for instance to allow coordination of manoeuvres);
- Information concerning specialized support chains (combat engineering, resupply,_logistics, maintenance etc);
- Exchange of combat status of own and neighbouring units (such as operative readiness, energy, etc);
- Information allowing hybrid applications with civil or other partners (e.g., police).

These capabilities should encompass data filtering in order to send the adequate information to the adequate friendly European partners' elements on the battlefield. They should also take into account issues like meta data, data lake, information exchange gateways, national regulations regarding the sharing of information/software and algorithms as well as data centric security.

These collective capabilities should be resilient in a global navigation satellite system (GNSS) denied environment or, where the electromagnetic spectrum is contested.

Data fusion (using more seamless data exchange, data fusion and possibly collective data processing) in order to share and improve a common situational awareness (and thus increase national resources) and allow coordinated manoeuvres:

- Enhanced collaborative blue force tracking: geolocalisation can be refined through data fusion (for instance through triangulation between multiple observations or sensors);
- Collaborative detection – reconnaissance – identification – localization and tracking: refine enemy force understanding through data fusion;
- Collaborative environment modelling: refine and extend environment models through data fusion. This function could also include coordination to map the environment (observation can also apply more broadly to quickly explore a larger area with different platforms from several countries) or to define the best observation sectors for battlefield surveillance, potentially using remote sensors such as UAVs;

- Collaborative scene analysis (including for instance change analysis or detection of abnormal events);
- Enemy tactical picture: to be refined through automated data fusion;
- Tactical situation sharing (such as RGP);
- Command and control (C2) coordination tools: C2 can be coordinated to achieve collaborative manoeuvres within the coalition and if it is associated to artificial intelligence (AI) to help plan itineraries and analyse the situation.

Technical solutions should be based on:

- Flexible middleware architectures for various levels of integration of multinational forces within combined network-enabled operations allowing an efficient (e.g., seamless, flexible, cyber protected) communication network combined with a unified battle management system to be progressively integrated into a framework of secured combat cloud as a key game changer[55];
- Scalable architecture to adapt to the several missions and working levels;
- The middleware should allow to control the electromagnetic and data signature of the unit;
- Standard interfaces to guarantee the interoperability with the existing and new platforms. A robust and open on-board platform network;
- Automated data fusion (e.g., image processing, sensor fusion, multi-criteria optimization, meta data management, simultaneous multi sensor usage) and HMI;
- Modern and innovative HMI able to integrate data coming from:
    - Various kinds of sensors (e.g., optronics, warning systems, navigation sensors);
    - Various kinds of effectors.

Standards and norms:

From a technical point of view, collaborative warfare should also meet the FMN criteria and therefore, be compatible with all other systems meeting the FMN criteria.

Other enabling standards and norms should be included like NGVA (NATO Generic Vehicle Architecture) as well as the European ESSOR (European Secure Software defined Radio) coalition waveforms for software defined radios. For sharing of sensor data within and among platforms architecture for sensor systems such as NATO STANAG 4822 Land DAS Architectures should also be addressed. Furthermore, standards on identification of friend or foe functionality should be considered.

Based on the coalition services identified for land collaborative combat, the proposal shall identify potential technical and operational requirements and long-term guidelines for future evolutions of these norms and standards.

[55] Allowing subsidiarity and data filtering to transfer only the more useful and adequate information within the network.

Furthermore, it is necessary to keep in consideration the ethical implication concerning the employment of e.g., AI and RAS (Robotics and Autonomous Systems) and the need to be in line with the mission rules of engagement and legislation used for military application.

First collaborative actions (as a first step for the present call since it implies distant request to other nations' assets and thus sharing part of national resources to improve coalition operations):

- Handover of ISR robotic assets, possibly including semi-autonomous coordination of multi-national UxV for information collection purpose.

Next collaborative actions (to be covered by a follow-up action, not part of this call topic):

- Integrate the most mature functions into target systems (e.g., vehicles or UxV associated with specific battlefield management systems and radios), which would be defined by the pMS;
- pursue the maturation of prospective functions;
- study new functions dedicated to new use cases for common collaborative action beyond information sharing and observation (e.g., collaborative fires or collaborative protection).

Expected impact

- Enable secured network-enabled operations relying on the distribution of basic warfighting functions (e.g., observation leading to ISR, command & control, fire management, protection) among different combat systems;
- Rebuild a credible deterrent in terms of land combat capability, by introducing in shortest possible time advanced solutions for collaborative combat within coalitions;
- Introduce new innovative collaborative combat technologies and capabilities that can be adapted to various manned or unmanned platforms;
- Provide a governmental EU agreed framework that industry can use to build state of the art and highly innovative systems dedicated to collaborative/federated land combat for emerging and future capability needs;
- Provide solutions that solve emerging/future capability needs of several Member States and Norway with maximum commonality and modularity;
- Increase strategic autonomy of EU concerning technologies and products.

EDF-2022-DA-NAVAL-MSAS: Medium-size semi-autonomous surface vessel

Objectives

The goal is to study, design, prototype and test a medium-sized semi-autonomous surface vessel (MSAS) with at least an ISR[56] modular mission payload.

Medium-sized should be understood as a vessel that can host the designed mission modules, be optionally manned based on the level of ambition described in scope and functional requirements sections of this call text.

[56] Intelligence, Surveillance, Reconnaissance.

Semi-autonomy should be understood as a primarily option to operate the platform and mission modules remotely. Due to the constrains related to certain use cases (e.g., legal restrictions, security and safety aspects, non-permissive electromagnetic environment), the vessel should be operable using a minimal manning to oversee the automated functions and/or operate mission modules and/or weapons on-board. Requirements linked to human factors when the vessel is manned (e.g., on-board facilities) and subsequent impact in the design (e.g., size) should be considered.

The main results should be a core platform designed to support unmanned operations with optional/minimal manning, 24/7 littoral operations, ISR missions, and providing versatility in terms of capability packages at affordable cost.

The use of a best practice[57] as guidance to terminology and definitions regarding Unmanned Maritime Systems (UMS) is advisable.

As part of the exploitation actions considered by a potential dissemination and communication strategy for sharing information and results towards external stakeholders, a live demonstration focused, in particular, on the Navies of Member States and associated countries should be considered.

The mission modules to be considered are:

a. ISR as part of the core platform (design & prototype)

b. Naval Mine Warfare (NMW) (design)

c. Anti-surface Warfare (ASuW) (design)

d. Anti-submarine Warfare (ASW) (design)

Scope and types of activities

Scope

The proposal must address challenges at three levels:

LEVEL 1: Digital and environmental transformation

Proposals must facilitate the cross-fertilization between civil and defence sectors and intend to speed up the adoption of novel autonomy and green energy technologies in the naval domain by developing a MSAS that European navies can begin taking into service starting from the end of this decade.

LEVEL 2: Confined littoral operating environment

A littoral force of smaller and many, rather than larger and few, tends to offer greater flexibility in crisis and conflict, which is why a MSAS has advantages in confined littoral operating environment.

LEVEL 3: Modularity and affordability

Mission dedicated naval assets are typically too expensive and unaffordable for small navies to cover sufficiently board range of coastal naval capabilities. To fill the capability gaps, decisive steps need to be taken towards innovative solutions that are more cost-efficient, affordable and lean in terms of manning. This is possible through modularity, automation/autonomy of certain functions, and through design choices

[57] Like, for instance, the guide for UMS handling, operations, design and regulations developed by the SARUMS (Safety and Regulations for European UMS) group in the context of the European Defence Agency UMS programme.

that reduce production and life-cycle costs. Where possible, mission module designs should take stock of existing technologies/components rather than designing completely new solutions.

Type of activities

The following table lists the types of activities which are eligible, and whether they are mandatory or optional *(see Article 10(3) EDF Regulation)*:

Types of activities (art 10(3) EDF Regulation)		**Eligible?**
(a)	Activities that aim to create, underpin and improve knowledge, products and technologies, including disruptive technologies, which can achieve significant effects in the area of defence (**generating knowledge**)	No
(b)	Activities that aim to increase interoperability and resilience, including secured production and exchange of data, to master critical defence technologies, to strengthen the security of supply or to enable the effective exploitation of results for defence products and technologies (**integrating knowledge**)	Yes (optional)
(c)	**Studies**, such as feasibility studies to explore the feasibility of new or upgraded products, technologies, processes, services and solutions	Yes (mandatory)
(d)	**Design** of a defence product, tangible or intangible component or technology as well as the definition of the technical specifications on which such a design has been developed, including any partial test for risk reduction in an industrial or representative environment	Yes (mandatory)
(e)	**System prototyping**[58] of a defence product, tangible or intangible component or technology	Yes (mandatory)
(f)	**Testing** of a defence product, tangible or intangible component or technology	Yes (mandatory)
(g)	**Qualification**[59] of a defence product, tangible or intangible component or technology	Yes (optional)
(h)	**Certification**[60] of a defence product, tangible or intangible component or technology	Yes (optional)
(i)	Development of technologies or assets **increasing efficiency** across the life cycle of defence products and technologies	Yes (optional)

The following tasks must be performed as part of the mandatory activities of the project:

- Studies:
    - Technical feasibility studies must include, at least, the following aspects:

[58] 'System prototype' means a model of a product or technology that can demonstrate performance in an operational environment.

[59] 'Qualification' means the entire process of demonstrating that the design of the product, component or technology meets the specified requirements, providing objective evidence by which particular requirements of a design are demonstrated to have been met.

[60] 'Certification' means the process by which a national authority certifies that the product, component or technology complies with the applicable regulations.

    - core components (e.g., autonomy including COLREG[61] compliant re-routing algorithms);
    - secure communications, and command and control (C2);
    - sensor data and other information management principles (e.g., storage and handling on-board, outside, both);
    - mission modules and their integration with the core platform;
    - cyber security requirements;
    - Safety of Navigation assessment, and certifiability according to national and international laws at sea;
    - logistic and user's package, including emergency procedures.

- Design:
  - System architecture.
  - Core platform, including ISR module.
  - Autonomy package.
  - Control station (equipment needed for remote/autonomous monitoring/control of MSAS).
  - Secure communication suit (e.g., internal, seashore, sea-sea).
  - Mission modules and mission modules integration.
- Prototyping:
  - Core platform with all key components, including ISR module.
  - Control station (equipment needed for remote/autonomous monitoring/control of Platform).
- Testing:
  - Components and system integration.
  - Trials in harbour and at sea.

Functional requirements

(1) General

a. Suitable for operating in harsh marine environments with large temperature variations from weather decks to machinery spaces with long mean time between repairs.

b. Capable of at least 2 000 nautical mile and/or 10 days self-sustained operations at 10 knots. Although the speed should be reliant on hull form,

[61] Convention on the International Regulations for Preventing Collisions at Sea, 1972.

the selection of propulsion plant and propelling system should consider reaching minimum 20 knots at maximum RPM[62] configuration.

c. Along with conventional combustion engine, proposals should consider electrical propulsion, Air Independent Propulsion (AIP), other alternative means (e.g., fuel cells) and/or advanced alternate fuels, as well as an optimal management of the integrated propulsion energy system.

d. The MSAS should be deployable, including by means of sealift, and capable of a sustained deployment, operating independently or as integral part of a naval task group.

e. The conceptual approach to the logistic and user’s package should consider advanced techniques related to system diagnostics, and capable of making conditional prognoses. Reduction of cost and time in production and in-service support should be taken into account from design.

f. Appropriate measures through its design or other means should be considered to reduce all facets of visual characteristics, electronic emissions and own signature, including the monitoring and reduction of radar, acoustic, infrared and magnetic signatures

g. The system should consider AI[63] algorithms for automatic situational awareness, threat identification and behavioural analysis. Without prejudice of the man-in-the-loop condition when required, those AI algorithms should improve decision-making in real-time without the intervention of the control station.

h. A self-defence weapons suit should be considered as part of the core platform. Any specific mission module (e.g., ASuW, ASW) should incorporate specific weapons as required by the concerned mission.

i. The option of standoff operations, cooperating with, or deployed from the MSAS, should be also considered. This could result in making the MSAS a remote-controlled data hub platform comprised of smaller USVs[64] and/or UUVs[65] and the MSAS operating as a rely-station to extend the operating radius.

(2) Positioning, Guidance, Navigation and Control

a. Alongside the encrypted (military) GNSS[66], an alternative positioning system should be considered, in order to provide redundancy and positional reliability in a GNSS denied environment.

b. Continuous generation and updating smooth, feasible and optimal trajectory commands to the control system according to the information provided by the navigation system, assigned missions, vessel capability and environmental conditions.

c. Identification of USV's current and future states (i.e., position, orientation, speed, acceleration) and their surrounding environment based on past and current states of the USV, also environmental information (e.g., winds, currents) obtained from sensors.

[62] Revolutions per minute.

[63] Artificial Intelligence.

[64] Unmanned Surface Vehicle.

[65] Unmanned Underwater Vehicle.

[66] Global Navigation Satellite Systems.

d. Control system to determine the proper control forces and moments to be generated, in conjunction with instructions provided by the guidance and navigation system, while satisfying desired control objectives.

(3) Autonomy package

a. Without excluding and fully compatible with a manned operation mode to be used when appropriate, an autonomy package should enable the MSAS to be operated until the Degree 3 in accordance with the 100th session of IMO's[67] Maritime Safety Committee (MSC 100): The M-SASV is remotely controlled without seafarers on board. The ship is supervised from another location and controlled and operated when necessary.

b. It should enable the vessel to navigate autonomously, understand its environment, and be able to make decisions and to determine actions by itself for a safe navigation under supervision. Sensors could be added to meet the need for autonomy.

c. In particular, it should allow MSAS to transit out of harbour, follow a mission pattern in a designated area for a designated period.

d. It should enable to control the proper functioning of the equipment, systems and facilities on-board, taking the necessary actions to protect them.

e. Each mission module should consider an unmanned operating mode enabling at least to operate the mission module remotely.

(4) Secure communications suite

MSAS should include a communications suite in order to allow for secure, real-time, automated two-ways connexion between the control station and both the core platform and on-board mission module, to guarantee as required, the proper governance of the vessel and the execution of the mission.

(5) ISR module (sensor suit)

a. MSAS should include a sensor suit equipping the core platform as needed to fulfil an ISR mission. Any other specific mission module could benefit of the outputs of this sensors suite and should complement it as needed.

b. Information gathered by on-board sensors (e.g., radar, EO/IR68) should be transmitted automatically via secure communications, to the control station. It should be possible to filter sensor information sent from the platform to the control station in accordance with pre-set criteria.

c. Capable of successful undertaking of surveillance tasks such as patrol and search. Sensors on-board should be capable of all weather, day/night operations in extreme climate and littoral operating environment.

d. A radar system capable of detecting surface targets with parameters characteristic in coastal areas ranging from Low Observable (LO) to major surface combatant and air targets with parameters ranging from either slow moving or loitering Remotely Piloted Aircraft System (RPAS) to fast moving stealthy combat air targets, should be considered

[67] International Maritime Organization.

[68] Electro optical/infrared.

e. Electronic support measures (ESM) should be considered.

(6) Other specific mission modules

a. Specific mission modules should be standardised to the maximum extent to reduce specific design requirements related to their integration in the MSAS, and to reduce the time of reconfiguration of the mission profile of the MSAS.

b. The NMW module should support as a minimum, naval mining operations. The feasibility of supporting naval mine countermeasures (NMC), mine hunting, minesweeping or both, should be evaluated during the study phase, taking into account ongoing dedicated programmes. The option of standoff NMC operations, deployed from the MSAS, should be also explored.

c. ASuW module should be capable to engage surface targets in such manner that out-of-action effect is achievable against a large defended surface target. The MSAS should become a weapon carrier integrated into a wider C4ISR69 network. The operation of the weapons system should still require a man-in-the-loop for engagement. Engagement of air targets should be limited to self-defence.

d. ASW module should consist of sensors and effectors to detect, locate, classify, track, and engage as needed, sub-surface targets by using passive and/or active acoustic devices at sufficient range. Innovative acoustic sensors for the detection of submarine and/or incoming torpedoes should be considered. Operation of the weapons system should still require a man-in-the-loop for engagement.

(7) Cyber security

Considering MSAS heavy reliance on software and connectivity, an improved protection against cyber threats should be considered, in particular as regards:

- Navigation and control systems communicating with shore-based or naval task group networks;
- Control systems monitoring the MSAS condition;
- Secure communication systems, gaining access to ship’s GNC[70] or other systems/subsystems via radio, satellite or wireless means, including the data exchange interface with on-board or shore-based control station;
- Machinery and propulsion systems;
- Launching and recovery systems.

Expected impact

- A new affordable medium-sized naval vessel class especially suitable for small and medium sized navies, and for larger navies for specific missions, depending on mission module configuration.
- Mission tailorable open architecture concept to facilitate operational versatility.

[69] Command, Control, Communications, Computers, Intelligence, Surveillance and Reconnaissance.

[70] Guidance, navigation and control.

- Modular design to facilitate support in congested spaces.
- Unmanned naval operations, in particular ISR, with man-in-the-loop and lean manning when needed, ensuring increased crew protection and 24/7 operational mode.
- Reduced environmental footprint.

EDF-2022-DA-NAVAL-NCS: Naval Collaborative Surveillance

Objectives

General objective

In the context of a changing geopolitical landscape, European Military Forces are facing new and evolving threats that are smaller, faster and more diverse, with increased manoeuvrability, like for instance Ballistic Missiles (BMs), Hypersonic Glide Vehicles (HGV) and Hypersonic Cruise Missiles (HCM), and swarmed attacks in a sensor adverse environment (e.g., stealth target, high target mix, environmental clutter, electronic attack).

Anti-Air Warfare (AAW) in the naval domain requires new technological developments to ensure lasting superiority at sea of EU naval surface vessels. Successful engagement to counter new threats can only be done by significantly reducing times as regards detection, tracking, identification and engagement.

EU navies already operate a variety of high-end sensors and weapons controlled by several combat management system, interconnected through Tactical Data Links (TDL) and other communication means, or have these under development. However, communications used nowadays (e.g., TDL 16/22) do not provide the speed, precision, configuration and update rate that enable successful engagements of future threats. Key challenge is to move from these existing capabilities to a naval collaborative surveillance ability in the Above Water Warfare (AWW) domain, based on real-time Plot Level Data Exchange and Fusion (PLDEF), emanating from diverse and heterogeneous platforms (ships or aerial) and relying on adequate and resilient communication means.

This new Naval Cooperative Surveillance (NCS) capability is considered as a first step and the basis for a capability on effector coordination (i.e., Force Threat Evaluation and Weapon Assignment) and Naval Collaborative Engagement (NCE).

Specific objective

The objective is to develop a full NCS capability allowing a better tactical situational awareness shared within a coalition, in terms of performances (e.g., coverage, robustness, accuracy of the information produced) and architecture resilience (e.g., degraded combat system, sensor failure, sensor jammed, loss of telecommunications).

It must consist in particular, in defining an EU NCS protocol/interface standard for real time exchange of raw data originated from sensors (plot level), thus facilitating the AWW operations within a coalition of EU naval and air assets. It must consist, as well, in developing processing functions and algorithms to use the data exchanged through the protocol/interface standard. The NCS will achieve a more effective elaboration of the tactical picture, through plot merging, tracking, identification, etc. Such data processing functions and algorithms could be developed either jointly or nationally. They must take the form of demonstrators and prototypes, which will be verified via demonstrations and testing. Further national implementation and deployment must comply with national legacies and strategies.

Furthermore, it is expected that the NCS has to be used in Global Navigation Satellite System (GNSS) denied areas. Therefore, the proposed NCS could also include a GNSS-independent mode that ensures successful operation when GNSS is vulnerable or unreliable. This GNSS-independent mode must result in minimal impact on the engageability of the tracks, still allowing for a NCE capability.

Scope and types of activities

Scope

The development of the NCS capability (i.e., NCS protocol/interface standard and data processing functions and algorithms) must be incremental. The following three broad levels of capability could be considered:

LEVEL 1: Define the NCS capability for plot exchange

This level 1 must define an EU protocol/interface standard that will allow European units within a naval force to share raw detection data in order to enrich the tactical situation. Each unit must perform its own tracking and fusion within NCS through national software modules. In this level also the GNSS-independent mode could be investigated, developed and tested.

This definition of the protocol/interface standard must be validated on board within real environments considering fast manoeuvring objects. Potential improvements will feedback the protocol/interface standard definition after such trials.

LEVEL 2: Extend to air assets and develop advanced NCS functions for situational awareness

This level 2 must extend the capability and the already defined protocol/interface standard to include air platforms with their own sensors, including unmanned platforms.

At this level, advanced functions and processing to set-up a better and unambiguous tactical situation, including identification and prevention of duplication of targets must be developed. New algorithms to select and prioritize plot dissemination within the network, to avoid data saturation of the network, must be defined and tested.

Coalition units might also operate TDL while embarking the new NCS capability. The coexistence of the tracks originated by the TDL network and the tracks originated by the new NCS capability, and the collaboration required between both for sharing common tactical situation awareness, must be studied.

Further national implementations and deployments should comply with national legacies and strategies.

LEVEL 3: Full advanced NCS capability

To improve the tactical situational awareness shared within the coalition, additional functions for the NCS capability must allow to:

- Handle unit(s) when entering/exiting the coalition network and other required network management functionalities.
- Prepare, and continuously update in real-time, the surveillance mission by planning operational unit(s) locations and movements, as well as task operational unit(s) while in operations within the coalition network.
- Include some level of sensor management, for example, to select the best combination of sensors available in the coalition for a given timeline per a

given cell of the surveillance space with the aim to optimize the quality of the tactical situation awareness and minimize communications workload.

A preliminary NCE capability, also known as Multi-Platform Engagement Capability (MPEC) that goes beyond the above-described concepts must be considered. Studies and first analysis on Launch-On-Remote and Engage-On-Remote, could be proposed as a follow-up paving the way to a European NCE capability.

Types of activities

The following table lists the types of activities which are eligible, and whether they are mandatory or optional *(see Article 10(3) EDF Regulation)*:

Types of activities (art 10(3) EDF Regulation)		**Eligible?**
(a)	Activities that aim to create, underpin and improve knowledge, products and technologies*,* including disruptive technologies, which can achieve significant effects in the area of defence (**generating knowledge**)	No
(b)	Activities that aim to increase interoperability and resilience, including secured production and exchange of data, to master critical defence technologies, to strengthen the security of supply or to enable the effective exploitation of results for defence products and technologies (**integrating knowledge**)	Yes (optional)
(c)	**Studies**, such as feasibility studies to explore the feasibility of new or upgraded products, technologies, processes, services and solutions	Yes (mandatory)
(d)	**Design** of a defence product, tangible or intangible component or technology as well as the definition of the technical specifications on which such a design has been developed, including any partial test for risk reduction in an industrial or representative environment	Yes (mandatory)
(e)	**System prototyping**[71] of a defence product, tangible or intangible component or technology	Yes (mandatory)
(f)	**Testing** of a defence product, tangible or intangible component or technology	Yes (mandatory)
(g)	**Qualification**[72] of a defence product, tangible or intangible component or technology	Yes (optional)
(h)	**Certification**[73] of a defence product, tangible or intangible component or technology	Yes (optional)
(i)	Development of technologies or assets **increasing efficiency** across the life cycle of defence products and technologies	Yes (optional)

The following tasks must be performed as part of the mandatory activities of the project:

- Studies:

[71] 'System prototype' means a model of a product or technology that can demonstrate performance in an operational environment.

[72] 'Qualification' means the entire process of demonstrating that the design of the product, component or technology meets the specified requirements, providing objective evidence by which particular requirements of a design are demonstrated to have been met.

[73] 'Certification' means the process by which a national authority certifies that the product, component or technology complies with the applicable regulations.

  - The evolutions of the EU protocol/interface standard required for each of the foreseen NCS capability levels 1, 2 and 3.

  - Inventory of the available and planned communication and network capacities and constraints which could be used in a coalition, with a view to propose the most appropriate architecture and interface definition, considering the evolution of communication capabilities over the next decade and with a view to identify potential new needs:

    - Data exchange needs must be characterized in terms of synchronization among participating units, time budget for data transfer, transmission rate, latency, discretion, range, confidentiality and resiliency.

    - The communication operation architecture and preliminary solutions must be identified based on considering different coalition deployment, threat and interoperability scenarios requirements. They must consider FMN (Federating Mission Networking) spirals and integration impact.

NB: Available and planned communication and network capability must be considered as an input to this project, which should focus on how to use currently available communication and network solutions in an optimal way. Thus, the design of new communication and network capabilities is out of the scope of this topic.

  - Additional, studies activities could focus on NCE functional analysis and preliminary engineering (pre-feasibility).

- Design:

  - Generic NCS architecture for levels of capability 1, 2 and 3

  - Common Data Model for levels of capability 1, 2 and 3

  - EU NCS protocol/interface standard for the exchange of surveillance data (e.g., plot, strobe) originated by radar, infrared search and tracking system, radar ESM (Electronic Support Measures), between sensors interconnected through appropriate communication means and network.

  - Processing functions and algorithms of the exchanged data, which could be developed either jointly or nationally; in order to optimise the sharing of data while maintaining the highest level of tactical situation quality and tracking.

NB: the topic also comprises the design of NCS protocol/interface standard and processing functions and algorithms related to the optimal use of available and planned communication and network capability. Such designs could be implemented either in NCS specific equipment (e.g., CMS – Combat Management System) or in network specific equipment (e.g., network management system). In the last case, the topic could be limited to the production of requirement documents or extended to actual implementation.

- Prototyping:

Equipment (hardware and software) implementing the required NCS protocol/interface standard, data processing functions and algorithms, and interfaces to be used as a model to test performance in a realistic operational environment.

- Testing:

Based on realistic operational scenarios, tests in real environments must consist of operating the prototype on-shore and at-sea. Trials with land platforms under synchronised simulated scenarios must be used extensively too, aiming to decrease costs and simulate future scenarios, which are difficult or impossible to implement at sea. While testing at sea, onshore or on platforms, each equipment (prototype) must create its own tactical situational awareness, and record the information products for further analysis. After testing completion, outcomes and feedback must be analysed to propose protocol changes when justified. Testing should involve a large number of actors (ships and air assets) from different Member States and associated countries, and take provisions for interoperability with NATO allies.

Functional requirements

The aim of the proposal should be to develop to an EU NCS for real time sharing of sensor data on plot level, showing the following main functional abilities:

- Develop a European NCS capability providing a dynamic and real-time sharing and fusion of heterogeneous raw data from naval and airborne sensors assets (potentially enhanced with land-based sensor information).

- Develop advanced management functions to achieve NCS and NCE, such as data transmission optimization, optimal positioning of naval assets, and dynamic management of multiple sensors.

- Optimize the overall NCS capability performance and resilience against advanced, evolving advanced threat set, like BMs, swarming, hypersonic targets or jamming.

- Prepare steps for further European collaborative Force Level capabilities including NCE.

The proposed NCS should support collaborative naval operations against modern threats and should be adaptable towards future threat evolutions.

The concept of operations for coordination of naval operations and provide naval support to joint and combined operations should be based on operational doctrines and systems of both Member States and associated countries, and strategic partners.

The architecture based on standards should be a non-intrusive and open for all Member States and associated countries.

The proposed solution should reuse previous works in this area as executed by contributing partners, in particular for demonstration and testing purposes.

Interoperability with allies, especially in the context of NATO, is a key priority, in relationship with the US Cooperative Engagement Capability (CEC). Furthermore, cooperation with the Maritime Theatre Missile Defence (MTMD) Forum should be sought where feasible. However, the proposal has to allow for growing on its own pace without any dependency on NATO, US or MTMD.

Expected impact

- A major steppingstone towards enhancing the strength of EU Naval Forces, contributing to European Strategic Autonomy and enhancing surface naval manoeuvrability and superiority.

- Significant reduction of the detection, recognition, identification and engagement times of combined defence while facing new and evolving air threats (e.g., smaller, faster and more diverse, and with increased manoeuvrability).

- Standardization to improve interoperability, and operational cooperation in coalition allowing assets utilization optimization, both leading to superiority of naval systems operated by EU navies in the AWW.

- Contribution to increase the industrial cooperation and integration of the EU defence companies including SMEs and mid-caps.

EDF-2022-DA-SIMTRAIN-MSSI: Modelling, simulation and simulator integration contributing to decision-making and training

Objectives

General objective

This proposal should lead to an enhanced EU military training and decision-making capability by connecting individual national systems through distributed solutions. Achieving the added benefit of sharing and pooling resources across EU through a shared ecosystem of simulation services. The goal of this initiative should be to establish a Distributed Synthetic Training and decision-making capability in Europe.

Specific objective

Simulation developers have produced various types of simulator and simulations. The challenge is to develop a flexible, scalable, on-demand simulation capability that can integrate legacy and new systems, a framework that integrate several simulators (of different types) or simulators' components (of different types) and should also contain command and control (C2), C4I[74] and Tactical Data Link assets in a unique platform and to foster the interoperability among them. In particular, the solution should rely on the Modelling & Simulation as a Service concept (MSaaS), to allow deployment of national-specific as well as EU-wide federation of simulation systems across Europe.

In our rapidly changing environment modelling and simulation (M&S) solutions need to enable decision making, evaluation of course of action by providing faster and more accurate information. The complexity of today's threats is showing the limitations of today's simulation systems in terms of number of entities being simulated, resolution and fidelity of the terrain and infrastructure and domains supported as well as their interoperability.

Additionally, it must enhance the capabilities and readiness of forces in the European context.

Scope and types of activities

Scope

The scope includes Studies, the design and development of a modular common technical framework, levering simulation services approach, which can meet the stated challenge and demonstrate the solution for use-cases in the training domain and in the decision support domain. The proposals must investigate, validate and demonstrate the baseline architecture and the supporting tools and processes for this enhanced military training and decision-making capability.

The proposals must address studies, such as to explore the feasibility of new or improved technologies, products, processes, services and solutions and the design

[74] Command Control Communication Computer and Information.

and development of new and integration of state-of-the-art technologies in training and decision-making using simulation systems.

A modular simulation environment, open systems-based design must allow a rapid response to new requirements, emerging cybersecurity compliance, and improved interoperability. It should support geographically separated commands/Nations and the complexity of multi-national operations that are focused on the strategic, operational and tactical levels and other operations and missions.

It must be adaptable to the different and new combat scenarios, operations and missions' environment and must support multi-domain operations, which models the conventional physical domains (for example land, maritime and air). It could as well use inputs from other new domains including space, cyber, and information, human and cognitive.

It must also facilitate the execution of analytical war-games for decision making at strategic and operational level.

It must demonstrate the capability how it could scale up to support the expected activities while modelling the behaviour of large number of entities over large areas and cooperate with a range of different simulation and real systems and platforms in a physically distributed environment.

It must study the feasibility of a simulation network, which should enable sharing and pooling of not only modelling and simulation assets, data sets and services, but also connectivity to existing legacy systems, existing simulation systems, real systems and platforms, national training and mission centres as well as operational EU or national networks like C2/C4ISR/Tactical Data Link.

The proposals must address training at the tactical level, the operational level, as well as the strategic level for support to decision-making, and the integration of different types of simulators.

Types of activities

The following table lists the types of activities which are eligible, and whether they are mandatory or optional *(see Article 10(3) EDF Regulation)*:

Types of activities (art 10(3) EDF Regulation)		**Eligible?**
(a)	Activities that aim to create, underpin and improve knowledge, products and technologies, including disruptive technologies, which can achieve significant effects in the area of defence (**generating knowledge**)	No
(b)	Activities that aim to increase interoperability and resilience, including secured production and exchange of data, to master critical defence technologies, to strengthen the security of supply or to enable the effective exploitation of results for defence products and technologies (**integrating knowledge**)	Yes (optional)
(c)	**Studies**, such as feasibility studies to explore the feasibility of new or upgraded products, technologies, processes, services and solutions	Yes (mandatory)
(d)	**Design** of a defence product, tangible or intangible component or technology as well as the definition of the technical specifications on which such a design has been developed, including any partial test for risk reduction in an industrial or representative environment	Yes (mandatory)

(e)	**System prototyping**[75] of a defence product, tangible or intangible component or technology	Yes (mandatory)
(f)	**Testing** of a defence product, tangible or intangible component or technology	Yes (optional)
(g)	**Qualification**[76] of a defence product, tangible or intangible component or technology	Yes (optional)
(h)	**Certification**[77] of a defence product, tangible or intangible component or technology	Yes (optional)
(i)	Development of technologies or assets **increasing efficiency** across the life cycle of defence products and technologies	Yes (optional)

The following tasks must be performed as part of the mandatory activities of the project:

- Studies:
  - The identification of user (training) requirements for the system, by engaging prospected end users and performing background studies. Elaborate common EU training and decision-making objectives to reflect the synthetic requirements.
  - The definition of use cases to focus the initial demonstration of the system. Concise and concrete use cases are used to eventually demonstrate the capabilities of the system, and the system of systems concept. This activity includes selection of assets needed for the use cases, such as infrastructure (networking) tools, simulators and analysis tools.
  - The identification of required solutions and standards. Many components for a system are already available and can be composed to implement the envisioned solution. Available solutions will be identified and evaluated for their applicability. Relevant standards for (simulation) connectivity and interoperability will be identified and applied.
  - The analysis of “use case” for training & exercises, Analysis of use cases with associated specificities for a deployment within Member States and associated countries;
  - Analysis of requirements and functionalities for connecting in-use and future national training, missions and CD&E[78] centres, analysis on how to integrate legacy simulators and mission and environment data;
  - Elaboration and recommend a Reference Architecture for distributed ecosystem based on the relevant interoperability standards from NATO and other standardization organisations (SISO/IEEE/OGC/ISO). (e.g.,

[75] ‘System prototype’ means a model of a product or technology that can demonstrate performance in an operational environment.

[76] ‘Qualification’ means the entire process of demonstrating that the design of the product, component or technology meets the specified requirements, providing objective evidence by which particular requirements of a design are demonstrated to have been met.

[77] ‘Certification’ means the process by which a national authority certifies that the product, component or technology complies with the applicable regulations.

[78] Concept Development and Experimentation.

High Level Architecture (HLA), NATO Reference Architectures (RA), Mission Training through Distributed Simulation (MTDS), C2 – Simulation Interoperability (C2SIM), NATO M&S as a Service (MSaaS).

- Elaborate and recommend the EU guidelines and business model for distributed corporation (e.g., governance), leveraging NATO MSaaS principles.

- Technology maturation and risk mitigation by developing technology demonstrators, especially on the following technologies:

    - Joint Forces Scenario Generator, including multi-domain computer generated forces with AI engines for realistic behaviour of OPFOR (Opposing Forces) units;

    - Cross Domain solutions that permit a Member State or Norway to access and use M&S services from another Member State with different classification domain;

- Analysis on how to ensure and realise IT-security and cyber-resilience capabilities: "Cybersecurity by Design" approach to minimize risks and threats associated with potential security failures and obviate risks against cyberattacks;

- Establish an overview of all relevant EU training and decision-making assets, which could eventually join this EU system of systems.

- Design:

    - Design of system solution architecture and develop interoperability requirements using Modelling and Simulation as a Service concept (MSaaS), follow-on of NATO NMSG[79] works, taking into account the use cases defined in the study phase, with a focus on efficiency and automation to create concurrent multi-domain and multi-service exercises; The goal is to obtain distributed simulation means for Mission Training through Distributed Simulation (MTDS) and decision making purposes whenever and wherever needed, able to run multiple simulations simultaneously by sharing and reusing resources (with efficient use of hardware), able to adapt rapidly to changing needs and able to reduce cost of employing simulation;

    - Identification, evaluation and selection of services available on the market (non-development items) and software design of services not available on the market (development items).

    - Simulation Network Design

    - Simulation Interoperability using several standards (e.g., NATO/ SISO /IEEE/ OGC / ISO standards).

    - Design for large-scale operation and interoperability. The blueprint is a system of systems and thus needs to cater for large number of participants at multiple geographically dispersed sites, and a heterogeneous collection of assets with various characteristics. This

[79] NATO Modelling and Simulation Group.

    activity aims to incorporate these characteristics into the reference design.

    - Integrate EU training and decision-making assets and organisations in this system of systems

    - Development of advanced scenarios.

    - The design of a defence product, tangible or intangible component or technology as well as the definition of the technical specifications on which such design has been developed which may include partial tests for risk reduction in an industrial or representative environment. Specifically:

        - The design of a reference architecture for the project and especially the area where interoperability needs to be improved and matured.

        - Technology prototype, including Modelling and Simulation as a Service concept (MSaaS), which enables sharing and pooling of not only synthetic assets and data sets and services, but also connectivity to existing legacy systems, existing simulation systems at different level of security classification and qualification.

- Prototype:

    - Integration of various technology modules, system integration and relevant trials

    - System integration and deployment to prove an Initial Operational Capability.

    - Integrate decision making.

The following tasks may be performed as part of the optional activities of the project:

- Testing and qualification

    - Components and system integration

    - Test an initial EU distributed ecosystem infrastructure, including a persistent secure network, with MSaaS, M&S Cloud servers, Exercise Portal, and common services.

    - Advanced scenario’s execution to test the environment/system

    - Test the integration of synthetic training and exercises (Use case)

Functional requirements

The capability to be developed should meet the following functional requirements:

(1) General

a. The system architecture shall be designed in accordance with the modularity principle in order to be expandable to future operational capabilities and to integrate modules and tools coming from multiple sources, allowing other EU Defence projects to be linked, integrated or implemented through this one.

b. Cybersecurity aspects must be taken into account along all project phases, from requirements capture to system design and implementation, in order to ensure adequate resilience, survivability and information protection.

c. Elaborate distributed During and After-Action Review (DAAR) to enable users to harvest the benefits of the system.

(2) Technological

a. State-of-the-art system, with modern, intuitive user interfaces supporting operators in all their operational, technical, training and decision-making needs. Usability should be the cornerstone of the system design allowing the rapid installation, administration, operation, training and decision making.

b. Adoption of an agile development methodology, increasing collaboration between software engineers and operational users, and exploring emerging information technology innovations to enable early delivery and continual improvement of Defence training and decision-making technical capabilities.

c. The architecture shall be designed in such a way that a large-scale exercise can take advantage of a distributed infrastructure across participating nations considering cybersecurity aspects

(3) Integration of simulators

a. The proposed system shall be able to create a wide variety of situations and scenarios to create new exercises to store, share and reuse simulation resources between different simulators and interoperate with others in a federation, using standard protocols.

b. The system should be able to operate in a network that include different communication systems (e.g., WAN[80], SATCOM[81]).

c. The system shall be able to work simultaneously in different security domains and handle the information security requirements to control the information flows between these domains and the integrated external systems.

d. The proposed system shall be based on a modern service-oriented architecture (SOA), leveraging on Modelling and Simulation as a Service paradigm, with an extensive use of open standards, allowing full compatibility with NATO and national systems, both military and civilian.

e. Dynamic, scalable and resilient, capable of easily integrating all the actors and nodes for each simulation scenario or application. This will be provided through Service Management & Control (SMC) services.

f. The system shall combine different kind of combat and support operations simulations (e.g., Artillery, Cavalry and Infantry, Maritime, Air, Close Air Support and logistics) with the aim to reach a full integration of them to perform computer-assisted exercises (CAX) and decision-making activities.

[80] Wide Area Network.

[81] SATellite COMmunications.

(4) Support to Decision-making

The proposed system shall be able to create a wide variety of situations and scenarios to create new exercises to store, share and reuse simulation resources between different simulators and interoperate with others in a federation, using standard protocols

(5) Other

a. Definition of an initial set of conventional and hybrid warfare scenarios representative of the EU operations and missions for simulation, training and decision making.

b. The system shall be able to integrate Virtual and Constructive simulation environments, including C2 systems, in order to build synthetic extension of the training and decision-making space, supporting combat preparation (e.g., Virtual Battlefield concept).

c. The system shall be open and adhere to standards to share (internal) data with Data analytics and AI

d. The system shall leverage machine learning, artificial intelligence (where possible) to support better decision making as well as generating behavioural models (civilian, military) and creating content (terrain, infrastructure).

e. Psychological, physiological and cognitive aspects, in terms of the behaviour and reactions of the personnel when facing simulated experiences (stress for instance), should also be taken into account in order to collect information and knowledge about how they will react to similar situations on the battlefield.

f. The system should facilitate the optimized data exploitation including simulation data standardisation and integration in order to facilitate AAR (After Action Review) and allow data analytics, predictive analytics and roadmap towards adaptive learning environments.

g. The system shall be able to support specified availability requirements providing an open, scalable, high availability and transparent failover architecture.

h. The development of a future simulation or integrated simulation system should take into consideration new possible technological improvements during the project, and at least (without excluding other options): simulation and communication equipment and infrastructure, in order to be able to exchange information between the Member States and Norway simulation centres and information systems. This may require the use of dedicated terrestrial networks and satellite links, hub infrastructure and terminals.

i. The infrastructure to setup dedicated simulation centres, including facilities for operators, data centres, and all the associated equipment (operators' equipment, voice / video communications, local communications, etc.)

Expected impact

The project is expected to:

- Increase of interoperability and efficient use of simulation systems thereby facilitating joint training and operations among armed forces of the EU Member States and Norway
- Deliver a prototype of TRL 6 (at least) and integrate simulation means provided by EU Member States and associated countries and reinforce interoperability between them.
- Create common reference simulation building blocks that will improve the capabilities of the European defence industry to develop and supply state of the art simulation systems.
- Reduce the cost of military missions, in particular in the training and preparation phase enabling of mission profiles that cannot be executed using conventional means or executed in areas outside MS and Norway.
- Generate an operational decision-making (constructive) environment to test and train Joint and Command Structures.
- Foster innovation and cooperation for stakeholders in the defence M&S domain and create an ecosystem to develop EU autonomous industrial segments for further industrialization phase.
- Foster exchange of datasets, scenarios and AI assets to accelerate development of capabilities of EU Member States and associated countries by promoting a collaboration network between EU Member States and Norway including academies, research centres and industries looking for synergies with civil initiatives.

3. Available budget

The available call budget is **EUR 510 000 000**.

Specific budget information per topic can be found in the table below.

Topic	Topic budget	Multi-topic with common budget envelope (common ranked list)	Fixed maximum number of projects
EDF-2022-DA-C4ISR-EC2: European command and control system	EUR 30 000 000	No	1
EDF-2022-DA-C4ISR-SOFC2: Deployable special operations forces multi-environment command post and C2 System	EUR 20 000 000	No	1
EDF-2022-DA-CYBER-CIWT: Cyber and information warfare toolbox	EUR 33 000 000	No	No

EDF-2022-DA-CYBER-CSIR: Cybersecurity and systems for improved resilience	EUR 27 000 000	No	No
EDF-2022-DA-SPACE-ISR: Innovative multi-sensor space-based Earth observation capabilities towards persistent and reactive ISR	EUR 40 000 000	No	1
EDF-2022-DA-SPACE-SBMEW: Space-based missile early warning	EUR 90 000 000	No	1
EDF-2022-DA-MATCOMP-SMT: Smart and multifunctional textiles	EUR 20 000 000	No	No
EDF-2022-DA-AIR-AEW: Airborne electronic warfare	EUR 40 000 000	No	1
EDF-2022-DA-GROUND-CGC: Collaborative combat for land forces	EUR 50 000 000	No	No
EDF-2022-DA-NAVAL-MSAS: Medium-size semi-autonomous surface vessel	EUR 65 000 000	No	1
EDF-2022-DA-NAVAL-NCS: Naval Collaborative Surveillance	EUR 65 000 000	No	1
EDF-2022-DA-SIMTRAIN-MSSI: Modelling, simulation and simulator integration contributing to decision-making and training	EUR 30 000 000	No	1

The availability of the call budget still depends on the adoption of the EU budget for the year 2023 by the EU budgetary authority.

We reserve the right not to award all available funds or to redistribute them between the call priorities, depending on the proposals received and the results of the evaluation.

4. Timetable and deadlines

Timetable and deadlines (indicative)	
Call opening:	21 June 2022
Deadline for submission:	24 November 2022 – 17:00:00 CET (Brussels)
Evaluation:	November 2022 - June 2023
Information on evaluation results:	June/July 2023

GA signature[82]:	July-December 2023

5. Admissibility and documents

Proposals must be submitted before the **call deadline** *(see timetable section 4)*.

Proposals must be submitted **electronically** via the Funding & Tenders Portal Electronic Submission System (accessible via the Topic page in the Search Funding & Tenders section). Paper submissions are NOT possible.

Proposals (including annexes and supporting documents) must be submitted using the forms provided *inside* the Submission System (⚠ NOT the documents available on the Topic page — they are only for information).

Proposals must be **complete** and contain all the requested information and all required annexes and supporting documents:

- Application Form Part A — contains administrative information about the participants (future coordinator, beneficiaries and affiliated entities) and the summarised budget for the project *(to be filled in directly online)*
- Application Form Part B — contains the technical description of the project *(to be downloaded from the Portal Submission System, completed and then assembled and re-uploaded)*
- mandatory annexes and supporting documents *(templates available to be downloaded from the Portal Submission System, completed, assembled and re-uploaded together with Application Form Part B)*:
    - detailed budget table
    - participant information (including previous projects, if any)
    - list of infrastructure, facilities, assets and resources
    - cofinancing declarations (if the requested EU grant does not cover the total eligible costs of the project)
    - actual indirect cost methodology declarations (if actual indirect costs used)
    - harmonised capability declarations (if the project covers design activities)
    - declarations on procurement intent and common specifications (if the project covers system prototyping or testing or qualification or certification activities)
    - ethics issues table
    - ownership control declarations.

Please note that the amounts entered into the summarised budget table (filled in directly online) must correspond to the amounts calculated in the detailed budget table. In case of discrepancies, the amounts in the online summarised budget table will prevail.

[82] In case of change in the management mode for a given action (see Section 3 of the EDF Work Programme), this timeframe may be different.

At proposal submission, you will have to confirm that you have the **mandate to act** for all applicants. Moreover, you will have to confirm that the information in the application is correct and complete and that the participants comply with the conditions for receiving EU funding (especially eligibility, financial and operational capacity, exclusion, etc). Before signing the grant, each beneficiary and affiliated entity will have to confirm this again by signing a declaration of honour (DoH). Proposals without full support will be rejected.

Your application must be **readable**, **accessible and printable**.

Proposals (Part B) are limited to maximum **100 pages** (counting the work package descriptions). Evaluators will not consider any additional pages.

You may be asked at a later stage for further documents *(for legal entity validation, financial capacity check, bank account validation, etc)*.

ℹ For more information about the submission process (including IT aspects), consult the Online Manual.

6. Eligibility

Eligible participants (eligible countries)

In order to be eligible, the applicants (beneficiaries and affiliated entities) must:

- be legal entities (public or private bodies)
- be established in one of the eligible countries, i.e.:
  - EU Member States (including overseas countries and territories (OCTs))
  - non-EU countries :
    - listed EEA countries ('EDF associated countries', *see* *list of participating countries*)
- have their executive management structure established in eligible countries
- must not be subject to control by a non-associated third country or non-associated third-country entity (unless they can provide guarantees – see Annex 2 - approved by the Member State or EDF associated country where they are established)

Beneficiaries and affiliated entities must register in the Participant Register — before submitting the proposal — and will have to be validated by the Central Validation Service (REA Validation). For the validation, they will be requested to upload documents showing legal status and origin.

Other entities may participate in other roles, such as associated partners, subcontractors, third parties giving in-kind contributions, etc *(see section 13)*.

⚠ Please note that, in EDF, subcontractors involved in the action[83] and associated partners must also comply with the above-listed conditions concerning establishment and control.

Associated partners which are not established in one of the eligible countries (or which are subject to control by a non-associated third country or non-associated

[83] 'Subcontractors involved in the action' means subcontractors with a direct contractual relationship to a beneficiary or affiliated entity, other subcontractors to which at least 10 % of the total eligible costs of the action are allocated, and subcontractors which may need access to classified information in order to carry out the project.

third-country entity) may however participate exceptionally if certain conditions are fulfilled *(not contravene EU and MS security and defence interests; consistent with EDF objectives; results not subject to control or restriction by non-associated third countries or non-associated third-country entities; no unauthorised access to classified information; no potential negative effects over security of supply of inputs which are critical for the project)*, subject to agreement by the granting authority and without any funding under the grant.

Specific cases

Natural persons — Natural persons are NOT eligible (with the exception of self-employed persons, i.e. sole traders, where the company does not have legal personality separate from that of the natural person).

International organisations — International organisations are not eligible, unless they are international organisations whose members are only Member States or EDF associated countries and whose executive management structure is in a Member State or EDF associated country.

Entities without legal personality — Entities which do not have legal personality under their national law may exceptionally participate, provided that their representatives have the capacity to undertake legal obligations on their behalf, and offer guarantees for the protection of the EU financial interests equivalent to that offered by legal persons[84].

Associations and interest groupings — Entities composed of members may participate as 'sole beneficiaries' or 'beneficiaries without legal personality'[85]. ⚠ Please note that if the action will be implemented by the members, they should also participate (either as beneficiaries or as affiliated entities, otherwise their costs will NOT be eligible).

Subcontractors involved in the action — Subcontractors with a direct contractual relationship to a recipient *(i.e. beneficiary or affiliated entity)*, other subcontractors to which at least 10 % of the total eligible costs of the action is allocated, and subcontractors which may need access to classified information in order to carry out the action.

EU restrictive measures — Special rules apply for certain entities *(e.g. entities subject to EU restrictive measures under Article 29 of the Treaty on the European Union (TEU) and Article 215 of the Treaty on the Functioning of the EU (TFEU)[86] and entities covered by Commission Guidelines No 2013/C 205/05[87])*. Such entities are not eligible to participate in any capacity, including as beneficiaries, affiliated entities, associated partners, subcontractors or recipients of financial support to third parties (if any).

ℹ For more information, *see Rules for Legal Entity Validation, LEAR Appointment and Financial Capacity Assessment*.

Consortium composition

Proposals must be submitted by minimum 3 independent applicants (beneficiaries; not affiliated entities) from 3 different eligible countries.

[84] See Article 197(2)(c) EU Financial Regulation 2018/1046.

[85] For the definitions, see Articles 187(2) and 197(2)(c) EU Financial Regulation 2018/1046.

[86] Please note that the EU Official Journal contains the official list and, in case of conflict, its content prevails over that of the EU Sanctions Map.

[87] Commission guidelines No 2013/C 205/05 on the eligibility of Israeli entities and their activities in the territories occupied by Israel since June 1967 for grants, prizes and financial instruments funded by the EU from 2014 onwards (OJEU C 205 of 19.07.2013, pp. 9-11).

Eligible actions and activities

Eligible actions and activities are the ones set out in section 2 above.

The following actions and activities are not considered as eligible for funding under this call:

- projects that do not implement the objectives set out in Article 3 of the EDF Regulation
- projects that do not concern new defence products or technologies or the upgrade of existing defence products or technologies
- projects that do not relate to at least one of the types of activities set out in Article 10(3) of the EDF Regulation
- projects that do not cover the mandatory types of activities set out in section 2
- projects that concern products and technologies whose use, development or production is prohibited by international law
- projects that concern the development of lethal autonomous weapons without the possibility for meaningful human control over selection and engagement decisions when carrying out strikes against humans (with the exception of the development of early warning systems and countermeasures for defensive purposes).
- projects where background or results:
  - would be subject to control or restriction by a non-associated third country or non-associated third-country entity, directly, or indirectly through one or more intermediate legal entities, including in terms of technology transfer
  - and, for pre-existing information (background), this would impact the results.

Projects should take into account the results of projects supported by other EU funding programmes. The complementarities must be described in the project proposals (Part B of the Application Form).

Projects must comply with EU policy interests and priorities *(such as environment, social, security, industrial and trade policy, etc)*.

Financial support to third parties is not allowed.

Geographic location (target countries)

Proposals must relate to activities taking place in the eligible countries *(see above).*

⚠ Please note that moreover, in EDF, only infrastructure, facilities, assets and resources which are located or held in an eligible country may be used. Other assets, infrastructure, facilities or resources may be used only exceptionally if certain conditions are fulfilled (*no competitive substitutes are readily available; not contravene EU and MS security and defence interests; consistent with EDF objectives; results not subject to control or restriction by non-associated third countries or non-associated third-country entities*), subject to agreement by the granting authority and without any funding under the grant.

Duration

Project duration:

- for all topics: between 12 and 48 months

Projects of longer duration may be accepted in duly justified cases. Extensions are possible, if duly justified and through an amendment.

Project budget

Project budgets (maximum grant amount):

- for all topics under this call: should not exceed the budget available for the topic (see table in section 3).

This does not however preclude the submission/selection of proposals requesting other amounts. The grant awarded may be lower than the amount requested.

Ethics

Projects must comply with:

- highest ethical standards (including highest standards of research integrity) and
- applicable EU, international and national law.

Proposals under this call will have to undergo an ethics review to authorise funding and may be made subject to specific ethics rules (which become part of the Grant Agreement in the form of ethics deliverables, *e.g. ethics committee opinions/notifications/authorisations required under national or EU law*).

Security

Projects involving classified information must undergo security scrutiny to authorise *funding* and may be made subject to specific security rules (detailed in a security aspects letter (SAL) which is annexed to the Grant Agreement).

Projects where the Member States of the participating beneficiaries and affiliated entities decide to establish a specific security framework under Article 27(4) of the EDF Regulation, will be subject to this specific security framework and classified foreground information (results) generated by the project will be under the originatorship of these Member States.

If no such specific security framework is set up by the signature of the grant agreement, the security rules will be governed by Commission Decision 2015/444[88] and its implementing rules[89].

These rules provide for instance that:

- projects involving information classified TRES SECRET UE/EU TOP SECRET (or equivalent) can NOT be funded
- classified information must be marked in accordance with the applicable security instructions in the SAL

[88] See Commission Decision 2015/544/EU,Euratom of 13 March 2015 on the security rules for protecting EU classified information (OJ L 72, 17.3.2015, p. 53).

[89] See Article 27(4) EDF Regulation.

- information with classification levels CONFIDENTIEL UE/EU CONFIDENTIAL or above (and RESTREINT UE/ EU RESTRICTED, if required by national rules) may be:
  - created or accessed only on premises with facility security clearing (FSC) from the competent national security authority (NSA), in accordance with the national rules
  - handled only in a secured area accredited by the competent NSA
  - accessed and handled only by persons with valid personnel security clearance (PSC) and a need-to-know
- at the end of the grant, the classified information must either be returned or continue to be protected in accordance with the applicable rules
- action tasks involving classified information may be subcontracted only with prior written approval from the granting authority and only to entities established in an EU Member State or in a non-EU country with a security of information agreement with the EU (or an administrative arrangement with the Commission)
- disclosure of classified information to third parties is subject to prior written approval from the granting authority.

Please note that facility security clearing may have to be provided before grant signature. The granting authority will assess the need for clearing in each case and will establish their delivery date during grant preparation. Please note that in no circumstances can we sign any grant agreement until at least one of the beneficiaries in a consortium has facility security clearing.

Further security recommendations may be added to the Grant Agreement in the form of security deliverables *(e.g. create security advisory group, limit level of detail, use fake scenario, exclude use of classified information, etc)*.

Beneficiaries must ensure that their projects are not subject to third-country/international organisation security requirements that could affect implementation or put into question the award of the grant *(e.g. technology restrictions, national security classification, etc)*. The granting authority must be notified immediately of any potential security issues.

ℹ More information on security aspects can be found in Annex 3.

7. Financial and operational capacity and exclusion

Financial capacity

Applicants must have **stable and sufficient resources** to successfully implement the projects and contribute their share. Organisations participating in several projects must have sufficient capacity to implement all these projects.

The financial capacity check will be carried out on the basis of the documents you will be requested to upload in the Participant Register during grant preparation *(e.g. profit and loss account and balance sheet, business plan, audit report produced by an approved external auditor, certifying the accounts for the last closed financial year, etc)*. The analysis will be based on neutral financial indicators, but will also take into account other aspects, such as dependency on EU funding and deficit and revenue in previous years.

The check will normally be done for all beneficiaries, except:

- public bodies (entities established as public body under national law, including local, regional or national authorities) or international organisations
- if the individual requested grant amount is not more than EUR 60 000.

If needed, it may also be done for affiliated entities.

If we consider that your financial capacity is not satisfactory, we may require:

- further information
- an enhanced financial responsibility regime, i.e. joint and several responsibility for all beneficiaries or joint and several liability of affiliated entities *(see below, section 10)*
- prefinancing paid in instalments
- (one or more) prefinancing guarantees *(see below, section 10)*

or

- propose no prefinancing
- request that you are replaced or, if needed, reject the entire proposal.

For more information, *see Rules for Legal Entity Validation, LEAR Appointment and Financial Capacity Assessment*.

Operational capacity

Applicants must have the **know-how, qualifications** and **resources** to successfully implement the projects and contribute their share (including sufficient experience in projects of comparable size and nature).

This capacity will be assessed together with the Implementation' award criterion, on the basis of the competence and experience of the applicants and their project teams, including operational resources (human, technical and other) or, exceptionally, the measures proposed to obtain it by the time the task implementation starts.

If the evaluation of the award criterion is positive, the applicants are considered to have sufficient operational capacity.

Applicants will have to show their capacity via the following information:

- general profiles (qualifications and experiences) of the staff responsible for managing and implementing the project.
- description of the consortium participants (including previous projects, if any).

Additional supporting documents may be requested, if needed to confirm the operational capacity of any applicant.

Public bodies, Member State organisations and international organisations are exempted from the operational capacity check.

Exclusion

Applicants which are subject to an **EU exclusion decision** or in one of the following **exclusion situations** that bar them from receiving EU funding can NOT participate[90]:

[90] See Articles 136 and 141 of EU Financial Regulation 2018/1046.

- bankruptcy, winding up, affairs administered by the courts, arrangement with creditors, suspended business activities or other similar procedures (including procedures for persons with unlimited liability for the applicant's debts)
- in breach of social security or tax obligations (including if done by persons with unlimited liability for the applicant's debts)
- guilty of grave professional misconduct[91] (including if done by persons having powers of representation, decision-making or control, beneficial owners or persons who are essential for the award/implementation of the grant)
- committed fraud, corruption, links to a criminal organisation, money laundering, terrorism-related crimes (including terrorism financing), child labour or human trafficking (including if done by persons having powers of representation, decision-making or control, beneficial owners or persons who are essential for the award/implementation of the grant)
- shown significant deficiencies in complying with main obligations under an EU procurement contract, grant agreement, prize, expert contract, or similar (including if done by persons having powers of representation, decision-making or control, beneficial owners or persons who are essential for the award/implementation of the grant)
- guilty of irregularities within the meaning of Article 1(2) of EU Regulation 2988/95 (including if done by persons having powers of representation, decision-making or control, beneficial owners or persons who are essential for the award/implementation of the grant)
- created under a different jurisdiction with the intent to circumvent fiscal, social or other legal obligations in the country of origin or created another entity with this purpose (including if done by persons having powers of representation, decision-making or control, beneficial owners or persons who are essential for the award/implementation of the grant).

Applicants will also be refused if it turns out that[92]:

- during the award procedure they misrepresented information required as a condition for participating or failed to supply that information
- they were previously involved in the preparation of the call and this entails a distortion of competition that cannot be remedied otherwise (conflict of interest).

8. Evaluation and award procedure

The proposals will have to follow the **standard submission and evaluation procedure** (one-stage submission + one-step evaluation).

An **evaluation committee** (assisted by independent outside experts) will assess all applications. Proposals will first be checked for formal requirements (admissibility, and eligibility, *see sections 5 and 6*). Proposals found admissible and eligible will be evaluated (for each budget envelope; *see section 3*) against the operational capacity and award criteria *(see sections 7 and 9)* and then ranked according to their scores.

[91] Professional misconduct includes: violation of ethical standards of the profession, wrongful conduct with impact on professional credibility, false declarations/misrepresentation of information, participation in a cartel or other agreement distorting competition, violation of IPR, attempting to influence decision-making processes or obtain confidential information from public authorities to gain advantage.

[92] See Article 141 EU Financial Regulation 2018/1046.

For proposals with the same score (within a budget envelope) a **priority order** will be determined according to the following approach:

> Successively for every group of *ex aequo* proposals, starting with the highest scored group, and continuing in descending order:
>
> 1) Proposals will be prioritised according to the scores they have been awarded for the criterion 'Excellence and potential of disruption'. When these scores are equal, priority will be based on scores for the criterion 'Innovation and technological development'. When these scores are equal, priority will be based on scores for the criterion 'Competitiveness. When these scores are equal, priority will be based on scores for the criterion 'Creation of new cross-border cooperation'
>
> 2) If necessary, any further prioritisation will be based on the number of Member States or EDF associated countries, in which applicants involved in the proposal are established

All proposals will be informed about the evaluation result (**evaluation result letter**). Successful proposals will be invited for grant preparation; the other ones will be put on the reserve list or rejected.

⚠ No commitment for funding — Invitation to grant preparation does NOT constitute a formal commitment for funding. We will still need to make various legal checks before grant award: *legal entity validation, financial capacity, exclusion check, etc*.

Grant preparation will involve a dialogue in order to fine-tune technical or financial aspects of the project and may require extra information from your side. It may also include adjustments to the proposal to address recommendations of the evaluation committee or other concerns. Compliance will be a pre-condition for signing the grant.

If you believe that the evaluation procedure was flawed, you can submit a **complaint** (following the deadlines and procedures set out in the evaluation result letter). Please note that notifications which have not been opened within 10 days after sending will be considered to have been accessed and that deadlines will be counted from opening/access *(see also Funding & Tenders Portal Terms and Conditions)*. Please also be aware that for complaints submitted electronically, there may be character limitations.

9. Award criteria

The **award criteria** for this call are as follows:

- **Excellence and potential of disruption (5 points)**
    - Excellence of the overall concept and soundness of the proposed approach for the solution, including main ideas, technologies and methodology
    - Compliance of the proposal with the objectives, scope and targeted activities), functional requirements and expected impact of the topic as set out in section 2
    - Extent to which the objective and expected outcome of the proposed project differs from (and represents an advantage at strategic, technological or defence operational level over) existing defence products or technologies, or has a potential of disruption in the defence domain

- **Innovation and technological development (5 points)**
  - Extent to which the proposal demonstrates innovation potential and contains ground-breaking or novel concepts and approaches *(e.g. new products, services or business and organizational models)*, new promising technological improvements, or the application of technologies or concepts previously not applied in the defence sector
  - Integration of existing knowledge and previous or ongoing R&D activities in the defence and/or civil sectors, while avoiding unnecessary duplication
  - Extent to which the innovations or technologies developed under the proposal could spin-off to other defence applications and products
- **Competitiveness (5 points)**
  - Foreseen competitive advantage of the product/technology/solution vis-a-vis existing or planned products/technologies/solutions across the EU and beyond, including consideration given to the balance between performance and cost-efficiency of the solution
  - Potential to accelerate the growth of companies throughout the EU, based on an analysis of the EU internal market and the global market place, indicating, to the extent possible, the size and the growth potential of the market it addresses, as well as expected volumes of sales both within and outside of the EU.
  - Strength of the IP strategy *(e.g. patents)* associated with the solution to support the competitiveness and growth of the applicant companies
- **EDTIB autonomy (5 points)**
  - Extent to which the proposed project will contribute to the autonomy of the European defence technological and industrial base (EDTIB) by increasing the EU’s industrial and technological non-dependency from third countries
  - Beneficial impact that the proposed activities will have on the strength of the European security of supply, including the creation of a new supply chain
  - Extent to which the project outcome will contribute to the defence capability priorities agreed by Member States within the framework of the Common Foreign and Security Policy (CFSP), and in particular in the context of the Capability Development Plan (EDA version releasable to the industry); where appropriate, extent to which the proposal addresses regional or an international priorities which serve the security and defence interests of the EU as determined under the CFSP and do not exclude the possibility of participation of Member States or EDF associated countries
- **Creation of new cross-border cooperation (5 points)**
  - Extent to which the proposed project will create new cross-border cooperation between legal entities established in Member States or EDF associated countries, in particular SMEs and mid-caps, especially

compared to former activities in the technological area of the call and taking into account the specificity of the market

- Planned future cross-border cooperation between legal entities established in Member States or EDF associated countries and cooperation opportunities created by the proposed activities

- Extent to which SMEs and mid-caps which cooperate cross-border participate substantially, and industrial or technological added value brought by them

- **Lifecycle efficiency (5 points)**

  - Improvement in terms of the efficiency across the lifecycle in comparison to existing solutions; for example, improvement in terms of cost-effectiveness by lower production, operational, maintenance, repair and overhaul or disposal costs and/or potential simplification of processes or combination with existing processes for procurement, maintenance and disposal.

- **Member State cooperation (5 points)**

  - The contribution to the further integration of the European defence industry throughout the Union through the demonstration by the recipients that Member States have undertaken to jointly use, own or maintain the final product or technology in a coordinated way.

- **Implementation (5 points)**

  - Effectiveness and practicality of the structure of the work plan (work breakdown structure), including timing and inter-relation of the different work packages and their components (illustrated by a Gantt chart, Pert chart or similar)

  - Usefulness and comprehensiveness of the milestones and deliverables of the project; coherence and clarity of the criteria for reaching the milestones, which should be measurable, realistic and achievable within the proposed duration

  - Appropriateness of the management structures and procedures, including decision-making mechanisms, to the complexity and scale of the project; quality of the risk management, including identification and assessment of the project specific critical risks, which could compromise the achievement of the stated project's objectives and detail of proposed risk treatments *(e.g. mitigation measures)*

  - Appropriateness of the allocation of tasks and resources between consortium members, ensuring that all participants have a valid and complementary role; allocation of the work share that ensures a high level of effectiveness and efficiency for carrying out the project.

Award criteria	Minimum pass score	Maximum score	Weighting
Excellence and potential of disruption	n/a	5	2
Innovation and technological development	n/a	5	1

Competitiveness	n/a	5	1
EDTIB autonomy	n/a	5	2
Creation of new cross-border cooperation	n/a	5	2
Lifecycle efficiency	n/a	5	1
Member State cooperation	n/a	5	1
Implementation	n/a	5	1
Overall weighted (pass) scores	**37**	**55**	N/A

Maximum points: 55 points.

There is no minimum pass score for individual criteria.

Overall threshold: 37 points.

Proposals that pass the overall threshold will be considered for funding — within the limits of the available budget (i.e. up to the budget ceiling). Other proposals will be rejected.

Only one solution will be funded (i.e. if there are two proposals covering the same solution, the higher ranked proposal will be selected).

10. Legal and financial set-up of the Grant Agreements

If you pass evaluation, your project will be invited for grant preparation, where you will be asked to prepare the Grant Agreement together with the EU Project Officer.

This Grant Agreement will set the framework for your grant and its terms and conditions, in particular concerning deliverables, reporting and payments.

The Model Grant Agreement that will be used (and all other relevant templates and guidance documents) can be found on Portal Reference Documents.

Starting date and project duration

The project starting date and duration will be fixed in the Grant Agreement *(Data Sheet, point 1)*. Normally the starting date will be after grant signature. Retroactive application can be granted exceptionally for duly justified reasons — but never earlier than the proposal submission date.

Project duration: *see section 6 above.*

Milestones and deliverables

The milestones and deliverables for each project will be managed through the Portal Grant Management System and will be reflected in Annex 1 of the Grant Agreement.

The following deliverables will be mandatory for all projects:

- progress reports (every 6 to 12 months, to be agreed during grant agreement preparation).

Form of grant, funding rate and maximum grant amount

The grant parameters *(maximum grant amount, funding rate, total eligible costs, etc)* will be fixed in the Grant Agreement *(Data Sheet, point 3 and art 5)*.

Project budget (maximum grant amount): *see section 6 above*.

The grant will be a budget-based mixed actual cost grant (actual costs, with unit cost and flat-rate elements). This means that it will reimburse ONLY certain types of costs (eligible costs) and costs that were *actually* incurred for your project (NOT the *budgeted* costs). For unit costs and flat-rates, you can charge the amounts calculated as explained in the Grant Agreement *(see art 6 and Annex 2 and 2a)*.

The costs will be reimbursed at the funding rate fixed in the Grant Agreement. This rate depends on the type of activities and participants *(see section 2)*.

Grants may in principle NOT produce a profit (i.e. surplus of revenues + EU grant over costs). Where the no-profit rule is activated in the Grant Agreement, for-profit organisations must declare their revenues and, if there is a profit, we will deduct it from the final grant amount *(see art 22.3)*.

Moreover, please be aware that the final grant amount may be reduced in case of non-compliance with the Grant Agreement *(e.g. improper implementation, breach of obligations, etc)*.

Budget categories and cost eligibility rules

The budget categories and cost eligibility rules are fixed in the Grant Agreement *(Data Sheet, point 3, art 6 and Annex 2)*.

Budget categories for this call:

- A. Personnel costs
  - A.1 Employees, A.2 Natural persons under direct contract, A.3 Seconded persons
  - A.4 SME owners and natural person beneficiaries
- B. Subcontracting costs
- C. Purchase costs
  - C.1 Travel and subsistence
  - C.2 Equipment
  - C.3 Other goods, works and services
- D. Other cost categories
  - D.1 Financial support to third parties
  - D.2 Internally invoiced goods and services
- E. Indirect costs

Specific cost eligibility conditions for this call:

- personnel costs:
  - average personnel costs (unit cost according to usual cost accounting practices):Yes

  - SME owner/natural person unit cost[93]: Yes

- subcontracting costs:
  - country restrictions for subcontracting costs: Yes, subcontracted work must be performed in the eligible countries
- travel and subsistence unit cost[94]: No (only actual costs)
- equipment costs:
  - depreciation + full cost for listed equipment
- other cost categories:
  - costs for financial support to third parties: not allowed
  - internally invoiced goods and services (costs unit cost according to usual cost accounting practices): Yes
  - PCP procurement cost: No
- indirect cost:
  - flat-rate: 25% of the eligible direct costs (categories A-D, except subcontracting costs, financial support to third parties and exempted specific cost categories, i.e. internally invoiced goods and services and PCP procurement costs)

  or

  - actual costs

    ⚠ The indirect cost method selected will be fixed for the project and cannot be changed lateron.
- VAT: non-deductible VAT is eligible (but please note that since 2013 VAT paid by beneficiaries that are public bodies acting as public authority is NOT eligible)
- other:
  - in-kind contributions for free are allowed, but cost-neutral, i.e. they cannot be declared as cost
  - kick-off meeting: costs for kick-off meeting organised by the granting authority are eligible (travel costs for maximum 2 persons, return ticket to Brussels and accommodation for one night) only if the meeting takes place after the project starting date set out in the Grant Agreement; the starting date can be changed through an amendment, if needed
  - project websites: communication costs for presenting the project on the participants' websites or social media accounts are eligible; costs for *separate* project websites are not eligible
  - eligible cost country restrictions: Yes, only costs for activities carried out in eligible countries are eligible

[93] Commission Decision of 20 October 2020 authorising the use of unit costs for the personnel costs of the owners of small and medium-sized enterprises and beneficiaries that are natural persons not receiving a salary for the work carried out by themselves under an action or work programme (C(2020)7715).

[94] Commission Decision of 12 January 2021 authorising the use of unit costs for travel, accommodation and subsistence costs under an action or work programme under the 2021-2027 multi-annual financial framework (C(2021)35).

– other ineligible costs: Yes, costs related to the use of assets, infrastructure, facilities or resources located or held outside the eligible countries are not eligible (even if their use was authorised, *see section 6*).

Reporting and payment arrangements

The reporting and payment arrangements are fixed in the Grant Agreement *(Data Sheet, point 4 and art 21 and 22)*.

After grant signature, you will normally receive a **prefinancing** to start working on the project (float of normally **55%** of the maximum grant amount; exceptionally less or no prefinancing). The prefinancing will be paid 30 days from entry into force/starting date/financial guarantee (if required) — whichever is the latest.

For projects of more than 18 months, there may be one or more **additional prefinancing payments** linked to a prefinancing report and one or more **interim payments** (with detailed cost reporting).

In addition, you will be requested to submit one or more progress reports not linked to payments.

Payment of the balance: At the end of the project, we will calculate your final grant amount. If the total of earlier payments is higher than the final grant amount, we will ask you (your coordinator) to pay back the difference (recovery).

All payments will be made to the coordinator.

⚠ Please be aware that payments will be automatically lowered if one of your consortium members has outstanding debts towards the EU (granting authority or other EU bodies). Such debts will be offset by us — in line with the conditions set out in the Grant Agreement *(see art 22)*.

Please also note that you are responsible for keeping records on all the work done and the costs declared.

Prefinancing guarantees

If a prefinancing guarantee is required, it will be fixed in the Grant Agreement *(Data Sheet, point 4)*. The amount will be set during grant preparation and it will normally be equal or lower than the prefinancing for your grant.

The guarantee should be in euro and issued by an approved bank/financial institution established in an EU Member State. If you are established in a non-EU country and would like to provide a guarantee from a bank/financial institution in your country, please contact us (this may be exceptionally accepted, if it offers equivalent security).

Amounts blocked in bank accounts will NOT be accepted as financial guarantees.

Prefinancing guarantees are formally NOT linked to individual consortium members, which means that you are free to organise how to provide the guarantee amount *(by one or several beneficiaries, for the overall amount or several guarantees for partial amounts, by the beneficiary concerned or by another beneficiary, etc)*. It is however important that the requested amount is covered and that the guarantee(s) are sent to us in time to make the prefinancing (scanned copy via Portal AND original by post).

If agreed with us, the bank guarantee may be replaced by a guarantee from a third party.

The guarantee will be released at the end of the grant, in accordance with the conditions laid down in the Grant Agreement.

Certificates

Depending on the type of action, size of grant amount and type of beneficiaries, you may be requested to submit different certificates. The types, schedules and thresholds for each certificate are fixed in the Grant Agreement *(Data Sheet, point 4 and art 24)*.

Liability regime for recoveries

The liability regime for recoveries will be fixed in the Grant Agreement *(Data Sheet point 4.4 and art 22).*

For beneficiaries, it is one of the following:

- limited joint and several liability with individual ceilings — *each beneficiary up* to their maximum grant amount
- unconditional joint and several liability — *each beneficiary up to the maximum grant amount for the action*

or

- individual financial responsibility — *each beneficiary only for their own debts*.

In addition, the granting authority may require joint and several liability of affiliated entities (with their beneficiary).

Provisions concerning the project implementation

Security rules: *see Model Grant Agreement (art 13 and Annex 5)*

Ethics rules: *see Model Grant Agreement (art 14 and Annex 5)*

IPR rules: *see Model Grant Agreement (art 16 and Annex 5):*

- background and list of background: Yes
- protection of results: Yes
- limitations to transfers and licensing: Yes
- rights of use on results: Yes
- for Research Actions: access to results for policy purposes: Yes
- for Research Actions: access to special report: Yes
- for Research Actions: access rights to further develop results: Yes

Communication, dissemination and visibility of funding: *see Model Grant Agreement (art 17 and Annex 5):*

- additional communication and dissemination activities: Yes

Specific rules for carrying out the action: *see Model Grant Agreement (art 18 and Annex 5):*

- specific rules for EDF actions: Yes
- specific rules for PCP Grants for Procurement: No

- place of performance obligation for PCP Grants for Procurement: No
- specific rules for Grants for Financial Support: No
- specific rules for blending operations: No.

Other specificities

n/a

Non-compliance and breach of contract

The Grant Agreement (chapter 5) provides for the measures we may take in case of breach of contract (and other non-compliance issues).

For more information, *see AGA — Annotated Grant Agreement*.

11. How to submit an application

All proposals must be submitted directly online via the Funding & Tenders Portal Electronic Submission System. Paper applications are NOT accepted.

Submission is a **2-step process**:

a) **create a user account and register your organisation**

To use the Submission System (the only way to apply), all participants need to create an EU Login user account.

Once you have an EULogin account, you can register your organisation in the Participant Register. When your registration is finalised, you will receive a 9-digit participant identification code (PIC).

b) **submit the proposal**

Access the Electronic Submission System via the Topic page in the Search Funding & Tenders section (or, for calls sent by invitation to submit a proposal, through the link provided in the invitation letter).

Submit your proposal in 2 parts, as follows:

- Part A includes administrative information about the applicant organisations (future coordinator, beneficiaries, affiliated entities and associated partners) and the summarised budget for the proposal. Fill it in directly online
- Part B and Annexes through a password-protected single zip archive:
  - Part B (description of the action) covers the technical content of the proposal. Download the mandatory word template from the Submission System, fill it in and add to the zip archive as a PDF
  - Annexes (*see section 5*). Download templates, and add to zip archive as PDFs (unless other format specified).

The zip archive must be submitted password-protected (using AES-256 encryption method), with a size of less than 100 MB. The password (and any other passwords used in the documents) must be communicated before the deadline for submission to the following email address: DEFIS-EDF-PROPOSALS-PWD@ec.europa.eu (together with the proposal ID and the name of the zip archive).

⚠ If your proposal includes **classified information**, please contact us at DEFIS-EDF-PROPOSALS@ec.europa.eu — well in time before the deadline, in order to arrange the delivery of the classified documents. Please be aware that such documents MUST NOT under any circumstances be submitted online though the Funding & Tenders Portal.

The proposal must keep to the **page limits** *(see section 5)*; excess pages will be disregarded.

Documents must be uploaded to the **right category** in the Submission System otherwise the proposal might be considered incomplete and thus inadmissible.

The proposal must be submitted **before the call deadline** (*see section 4*). After this deadline, the system is closed and proposals can no longer be submitted.

Once the proposal is submitted, you will receive a **confirmation e-mail** (with date and time of your application). If you do not receive this confirmation e-mail, it means your proposal has NOT been submitted. If you believe this is due to a fault in the Submission System, you should immediately file a complaint via the IT Helpdesk webform, explaining the circumstances and attaching a copy of the proposal (and, if possible, screenshots to show what happened).

Details on processes and procedures are described in the Online Manual. The Online Manual also contains the links to FAQs and detailed instructions regarding the Portal Electronic Exchange System.

12. Help

As far as possible, ***please try to find the answers you need yourself***, in this and the other documentation (we have limited resources for handling direct enquiries):

- Online Manual
- FAQs on the Topic page (for call-specific questions in open calls; not applicable for actions by invitation)
- Portal FAQ (for general questions).

Please also consult the Topic page regularly, since we will use it to publish call updates. (For invitations, we will contact you directly in case of a call update).

Contact

For individual questions on the Portal Submission System, please contact the IT Helpdesk.

Non-IT related questions should be sent to the following email address: DEFIS-EDF-PROPOSALS@ec.europa.eu.

Please indicate clearly the reference of the call and topic to which your question relates *(see cover page)*.

13. Important

⚠ **IMPORTANT**

- **Don't wait until the end —** Complete your application sufficiently in advance of the deadline to avoid any last minute **technical problems**. Problems due to last minute submissions *(e.g. congestion, etc)* will be entirely at your risk. Call deadlines can NOT be extended.
- **Consult** the Portal Topic page regularly. We will use it to publish updates and additional information on the call (call and topic updates).
- **Funding & Tenders Portal Electronic Exchange System —** By submitting the application, all participants **accept** to use the electronic exchange system in accordance with the Portal Terms & Conditions.
- **Registration —** Before submitting the application, all beneficiaries, affiliated entities, associated partners must be registered in the Participant Register. The draft participant identification code (PIC) (one per participant) is mandatory for the Application Form.

  If your project applies for the SME/Mid-cap bonuses, registration (draft PIC and SME self-assessment wizard) is also mandatory for all participants claiming SME/Mid-cap status (beneficiaries, affiliated entities and subcontractors involved in the action; *see section 2*).

  Moreover, registration (draft PIC) is required for entities that must submit an ownership control assessment declaration (beneficiaries, affiliated entities, subcontractors involved in the action and associated partners).
- **Consortium roles —** When setting up your consortium, you should think of organisations that help you reach objectives and solve problems.

  The roles should be attributed according to the level of participation in the project. Main participants should participate as **beneficiaries** or **affiliated entities**; other entities can participate as associated partners, subcontractors, third parties giving in-kind contributions. **Associated partners** and third parties giving in-kind contributions should bear their own costs (they will not become formal recipients of EU funding). **Subcontracting** should normally constitute a limited part and must be performed by third parties (not by one of the beneficiaries/affiliated entities). Subcontracting going beyond 30% of the total eligible costs per beneficiary/affiliated entity must be justified in the application and may be accepted by the granting authority if the topic is not subject to a fixed subcontracting limit *(see section 10)*.
- **Coordinator —** In multi-beneficiary grants, the beneficiaries participate as consortium (group of beneficiaries). They will have to choose a coordinator, who will take care of the project management and coordination and will represent the consortium towards the granting authority. In mono-beneficiary grants, the single beneficiary will automatically be coordinator.
- **Affiliated entities** — Applicants may participate with affiliated entities (i.e. entities linked to a beneficiary which participate in the action with similar rights and obligations as the beneficiaries, but do not sign the grant and therefore do not become beneficiaries themselves). They will get a part of the grant money and must therefore comply with all the call conditions and be validated (just like beneficiaries); but they do not count towards the minimum eligibility criteria for consortium composition (if any).
- **Associated partners** — Applicants may participate with associated partners (i.e. partner organisations which participate in the action but without the right to get grant money). They participate without funding and therefore do not need to be validated.

- **Consortium agreement** — For practical and legal reasons it is recommended to set up internal arrangements that allow you to deal with exceptional or unforeseen circumstances (in all cases, even if not mandatory under the Grant Agreement). The consortium agreement also gives you the possibility to redistribute the grant money according to your own consortium-internal principles and parameters (for instance, one beneficiary can reattribute its grant money to another beneficiary). The consortium agreement thus allows you to customise the EU grant to the needs inside your consortium and can also help to protect you in case of disputes.

- **Balanced project budget —** Grant applications must ensure a balanced project budget and sufficient other resources to implement the project successfully *(e.g. own contributions, income generated by the action, financial contributions from third parties, etc)*. You may be requested to lower your estimated costs, if they are ineligible (including excessive).

- **No-profit rule —** Grants may in principle NOT give a profit (i.e. surplus of revenues + EU grant over costs). Where the no-profit rule is activated in the Grant Agreement, this will be checked by us at the end of the project.

- **No double funding —** There is a strict prohibition of double funding from the EU budget (except under EU Synergies actions). Outside such Synergies actions, any given action may receive only ONE grant from the EU budget and cost items may under NO circumstances declared to two different EU actions.

- **Completed/ongoing projects —** Proposals for projects that have already been completed will be rejected; proposals for projects that have already started will be assessed on a case-by-case basis (in this case, no costs can be reimbursed for activities that took place before the project starting date/proposal submission).

- **Combination with EU operating grants —** Combination with EU operating grants is possible, if the project remains outside the operating grant work programme and you make sure that cost items are clearly separated in your accounting and NOT declared twice *(see AGA — Annotated Model Grant Agreement, art 6.2.E)*.

- **Multiple proposals —** Applicants may submit more than one proposal for *different* projects under the same call (and be awarded a funding for them).

  Organisations may participate in several proposals.

  BUT: if there are several proposals for *very similar* projects, only one application will be accepted and evaluated; the applicants will be asked to withdraw one of them (or it will be rejected).

- **Resubmission —** Proposals may be changed and re-submitted until the deadline for submission.

- **Rejection —** By submitting the application, all applicants accept the call conditions set out in this this Call Document (and the documents it refers to). Proposals that do not comply with all the call conditions will be **rejected**. This applies also to applicants: All applicants need to fulfil the criteria; if any one of them doesn't, it must be replaced or the entire proposal will be rejected.

- **Cancellation —** There may be circumstances which may require the cancellation of the call. In this case, you will be informed via a call or topic update. Please note that cancellations are without entitlement to compensation.

- **Language —** You can submit your proposal in any official EU language (project abstract/summary should however always be in English). For reasons of efficiency, we strongly advise you to use English for the entire application. If you need the call documentation in another official EU language, please submit a request within 10 days after call publication (for the contact information, see section 12).

- **Transparency —** In accordance with Article 38 of the EU Financial Regulation, information about EU grants awarded is published each year on the Europa website.

  This includes:
  - beneficiary names
  - beneficiary addresses
  - the purpose for which the grant was awarded
  - the maximum amount awarded.

  The publication can exceptionally be waived (on reasoned and duly substantiated request), if there is a risk that the disclosure could jeopardise your rights and freedoms under the EU Charter of Fundamental Rights or harm your commercial interests.

- **Data protection —** The submission of a proposal under this call involves the collection, use and processing of personal data. This data will be processed in accordance with the applicable legal framework. It will be processed solely for the purpose of evaluating your proposal, subsequent management of your grant and, if needed, programme monitoring, evaluation and communication. Details are explained in the Funding & Tenders Portal Privacy Statement.

Annex 1

EDF types of action

EDF uses the following actions to implement grants:

Research Actions

Description: Research Actions (RA) target activities consisting primarily of research activities, in particular applied research and where necessary fundamental research, with the aim of acquiring new knowledge and with an exclusive focus on defence applications.

Funding rate: 100%

Payment model: Prefinancing — (x) additional prefinancing payment(s) — (x) interim payment(s) — final payment

Development Actions

Description: Development Actions (DA) target activities consisting of defence-oriented activities primarily in the development phase, covering new defence products or technologies or the upgrading of existing ones, excluding the production or use of weapon.

Funding rate: variable per activity (rates depend on activity and bonuses for SME and mid-cap participation and PESCO)

Payment model: Prefinancing — (x) additional prefinancing payment(s) — (x) interim payment(s) — final payment

PCP Grants for Procurement

Description: PCP Grants for Procurement (PCP) target activities that aim to help a transnational buyers' group to strengthen the public procurement of research, development, validation and, possibly, the first deployment of new solutions that can significantly improve quality and efficiency in areas of public interest, while opening market opportunities for industry and researchers active in Europe. Eligible activities include the preparation, management and follow-up, under the coordination of a lead procurer, of one joint PCP and additional activities to embed the PCP into a wider set of demand-side activities.

Funding rate: variable (to be defined in the work programme)

Payment model: Prefinancing — (x) additional prefinancing payment(s) — (x) interim payment(s) — payment of the balance

Lump Sum Grants for Research Actions

Description: Lump Sum Grants (LS-RA) reimburse a general lump sum for the entire project and the consortium as a whole. The lump sum is fixed ex-ante (at the latest at grant signature) on the basis of a methodology defined by the granting authority (either on the basis of a detailed project budget or other pre-defined parameters). The lump sum will cover all the beneficiaries' direct and indirect costs for the project. The beneficiaries do not need to report actual costs, they just need to claim the lump sum once the work is done. If the action is not properly implemented, only part of the lump sum will be paid.

Lump Sum Grants for Research Actions cover the same type of activities as Research Actions and follow — where relevant — similar rules *(e.g. for funding rates, etc.)*.

Funding rate: 100%

Payment model: Prefinancing — (x) additional prefinancing payment(s) — (x) interim payment(s) — final payment

Lump Sum Grants for Development Actions

Description: Lump Sum Grants (LS-DA) reimburse a general lump sum for the entire project and the consortium as a whole. The lump sum is fixed ex-ante (at the latest at grant signature) on the basis of a methodology defined by the granting authority (either on the basis of a detailed project budget or other pre-defined parameters). The lump sum will cover all the beneficiaries' direct and indirect costs for the project. The beneficiaries do not need to report actual costs, they just need to claim the lump sum once the work is done. If the action is not properly implemented, only part of the lump sum will be paid.

Lump Sum Grants for Development Actions cover the same type of activities as Development Actions and follow — where relevant — similar rules *(e.g. for funding rates, etc)*.

Funding rate: variable per activity (rates depend on activity and bonuses for SME and mid-cap participation and PESCO)

Payment model: Prefinancing — (x) additional prefinancing payment(s) — (x) interim payment(s) — final payment

Framework Partnerships (FPAs) and Specific Grants (SGAs)

FPAs

Description: FPAs establish a long-term cooperation mechanism between the granting authority and the beneficiaries of grants. The FPA specifies the common objectives (action plan) and the procedure for awarding specific grants. The specific grants are awarded via identified beneficiary actions (with or without competition).

Funding rate: no funding for FPA

SGAs

Description: The SGAs are linked to an FPA and implement the action plan (or part of it). They are awarded via an invitation to submit a proposal (identified beneficiary action). The consortium composition should in principle match (meaning that only entities that are part of the FPA can participate in an SGA), but otherwise the implementation is rather flexible. FPAs and SGAs can have different coordinators; other partners of the FPA are free to participate in an SGA or not. There is no limit to the amount of SGAs signed under one FPA.

Funding rate: depending on the type: 100% or variable per activity

Payment model: Prefinancing — (x) additional prefinancing payment(s) — (x) interim payment(s) — final payment

Annex 2

Guarantees pursuant to Article 9(4) of the EDF Regulation

All calls under the EDF Programme are subject to ownership control restrictions, meaning that they exclude the participation of legal entities which are established in the EU territory or in an EDF associated country, but are controlled by a non-associated third country or non-associated third country legal entity.

Thus, for the purposes of participating in EDF actions, beneficiaries, affiliated entities, associated partners and subcontractors involved in the action must not be subject to control by a non-associated third country or non-associated third-country entity and undergo an ownership control assessment procedure before grant signature.

Entities that do not comply with this requirement may however exceptionally nevertheless participate, if they can provide guarantees approved by the Member State/EDF associated country in which they are established. Such guarantees must be provided at the latest by grant signature.

The guarantees must provide assurance to the granting authority that the participation of the entity will not contravene the security and defence interests of the EU and its Member States as established in the framework of the Common Foreign and Security Policy (CFSP) pursuant to Title V of the TEU, or the objectives set out in Article 3 of the EDF Regulation. They must also comply with the provisions on ownership and intellectual property rights (Articles 20 and 23 of the EDF Regulation).

They must in particular substantiate that, for the purposes of the action, measures are in place to ensure that:

- **control** over the legal entity is not exercised in a manner that would restrain or restrict its ability to carry out the action and to deliver results, that would impose restrictions concerning its infrastructure, facilities, assets, resources, intellectual property or knowhow needed for the purposes of the action, or that would undermine its capabilities and standards necessary to carry out the action

- **access** by a non-associated third country or non-associated third-country entity to sensitive information relating to the action is prevented and the employees or other persons involved in the action have national security clearance issued by a Member State or an EDF associated country, where appropriate

- **ownership** of the intellectual property arising from, and the results of, the action remain within the beneficiary or affiliated entity during and after completion of the action, are not subject to control or restriction by a non-associated third country or non-associated third-country entity, and are neither exported outside the EU/EDF associated countries nor accessible from outside the EU/EDF associated countries without the approval of the Member State/EDF associated country in which the legal entity is established and in accordance with the objectives set out in Article 3 of the EDF Regulation.

The guarantees may refer to the fact that the legal entity's executive management structure is established in the EU/EDF associated country or, if considered appropriate, to specific governmental rights in the control over the legal entity.

If considered appropriate by the Member State/EDF associated country, additional guarantees may be provided.

ℹ For more information, *see also* *Guidance on participation in DEP, HE, EDF and CEF-DIG restricted calls*.

Annex 3

Security aspects

Introduction

Pursuant to Article 27(4) of the EDF Regulation, in case the implementation of the grant involves the handling of classified information, Member States on whose territory the beneficiaries and affiliated entities are established must decide on the originatorship of the classified foreground information (results) generated in the performance of the project. For that purpose, those Member States may decide on a specific security framework for the protection and handling of classified information relating to the project and must inform the granting authority. Such a security framework must be without prejudice to the possibility for the granting authority to have access to necessary information for the implementation of the action.

If no such specific security framework is set up by those Member States, the security framework will be put in place by the granting authority in accordance with Decision 2015/444.

In either case, the security framework will be put in place at the latest by the signature of the Grant Agreement.

The applicable security framework will be detailed in the security aspect letter (SAL) which will be annexed to the Grant Agreement.

When you implement a classified grant, please bear in mind the following key rules.

Access to classified information

The creation, handling or access to information classified CONFIDENTIAL or SECRET (or RESTRICTED where required by national rules) on the premises of a participant is only possible if a valid Facility Security Clearance (FSC) at the appropriate level exists for the premises. This FSC must be granted by the National Security Authority (NSA/DSA) of the participant concerned.

The participant must hold a duly confirmed FSC at the appropriate level. Until a secured area is in place and accredited by the national NSA, the handling of classified information above RESTRICTED level on their premises is not allowed.

Access to and handling of classified information for the purposes of the project must be limited to individuals with a need-to-know and which are in possession of a valid personnel security clearance.

At the end of the Grant Agreement when EUCI is no longer required for the performance of the grant, the participant must return any EUCI they hold to the contracting authority immediately. If authorised to retain EUCI after the end of the grant, the EUCI must continue to be protected in accordance with Decision 2015/444.

Marking of classified information

Classified information generated for the performance of the action must be marked in accordance with the applicable security framework, as described in the SAL.

Grants must not involve information classified 'TRES SECRET UE/EU TOP SECRET' or any equivalent classification.

Other provisions

Where a participant has awarded a classified subcontract, the security provisions of the grant agreement must apply *mutatis mutandis* to the subcontractor(s) and their personnel. In such case, it is the responsibility of the participant to ensure that all subcontractors apply these principles to their own subcontracting arrangements.

All security breaches related to classified information will be investigated by the competent security authority and may lead to criminal prosecution under national law.

Table of equivalent security classification markings

	Secret	**Confidential**	**Restricted**
EU	SECRET UE/EU SECRET	CONFIDENTIEL UE/EU CONFIDENTIAL	RESTREINT UE/EU RESTRICTED
Austria	GEHEIM	VERTRAULICH	EINGESCHRÄNKT
Belgium	SECRET (Loi du 11 Dec 1998) or GEHEIM (Wet van 11 Dec 1998)	CONFIDENTIEL (Loi du 11 Dec 1998) or VERTROUWELIJK (Wet van 11 Dec 1998)	*(Note 1, see below)*
Bulgaria	СЕКРЕТНО	ПОВЕРИТЕЛНО	ЗА СЛУЖЕБНО ПОЛЗВАНЕ
Croatia	TAJNO	POVJERLJIVO	OGRANIČENO
Cyprus	ΑΠΌΡΡΗΤΟ ABR:(ΑΠ)	ΕΜΠΙΣΤΕΥΤΙΚΌ ABR:(ΕΜ)	ΠΕΡΙΟΡΙΣΜΈΝΗΣ ΧΡΉΣΗΣ ABR:(ΠΧ)
Czech Republic	TAJNÉ	DŮVĚRNÉ	VYHRAZENÉ
Denmark	HEMMELIGT	FORTROLIGT	TIL TJENESTEBRUG
Estonia	SALAJANE	KONFIDENTSIAALNE	PIIRATUD
Finland	SALAINEN or HEMLIG	LUOTTAMUKSELLINEN or KONFIDENTIELL	KÄYTTÖ RAJOITETTU or BEGRÄNSAD TILLGÅNG

France	SECRET SECRET DÉFENSE *(Note 2, see below)*	CONFIDENTIEL DÉFENSE *(Notes 2 and 3, see below)*	*(Note 4, see below)*
Germany ***(Note 5, see below)***	GEHEIM	VS - VERTRAULICH	VS - NUR FÜR DEN DIENSTGEBRAUCH
Greece	ΑΠΌΡΡΗΤΟ ABR:(ΑΠ)	ΕΜΠΙΣΤΕΥΤΙΚΌ ABR:(ΕΜ)	ΠΕΡΙΟΡΙΣΜΈΝΗΣ ΧΡΉΣΗΣ ABR:(ΠΧ)
Hungary	TITKOS!	BIZALMAS!	KORLÁTOZOTT TERJESZTÉSŰ!
Ireland	SECRET	CONFIDENTIAL	RESTRICTED
Italy	SEGRETO	RISERVATISSIMO	RISERVATO
Latvia	SLEPENI	KONFIDENCIĀLI	DIENESTA VAJADZĪBĀM
Lithuania	SLAPTAI	KONFIDENCIALIAI	RIBOTO NAUDOJIMO
Luxembourg	SECRET LUX	CONFIDENTIEL LUX	RESTREINT LUX
Malta	SIGRIET	KUNFIDENZJALI	RISTRETT
Netherlands	Stg. GEHEIM	Stg. CONFIDENTIEEL	Dep. VERTROUWELIJK
Poland	TAJNE	POUFNE	ZASTRZEŻONE
Portugal	SECRETO	CONFIDENCIAL	RESERVADO *(Note 6, see below)*
Romania	STRICT SECRET	SECRET	SECRET DE SERVICIU
Slovakia	TAJNÉ	DÔVERNÉ	VYHRADENÉ
Slovenia	TAJNO	ZAUPNO	INTERNO
Spain	RESERVADO *(Note 6, see below)*	CONFIDENCIAL	DIFUSIÓN LIMITADA
Sweden	HEMLIG	KONFIDENTIELL	BEGRÄNSAT HEMLIG

Notes:

Note 1 Belgium: ‘Diffusion Restreinte/Beperkte Verspreiding’ is not a security classification in Belgium. Belgium handles and protects RESTREINT UE/EU RESTRICTED information and classified information bearing the national classification markings of RESTRICTED level in a manner no less stringent than the standards and procedures described in the security rules of the Council of the European Union.

Note 2 France: Information generated by France before 1 July 2021 and classified SECRET DÉFENSE and CONFIDENTIEL DÉFENSE continues to be handled and protected at the equivalent level of SECRET UE/EU SECRET and CONFIDENTIEL UE/EU CONFIDENTIAL respectively.

Note 3 France: France handles and protects CONFIDENTIEL UE/EU CONFIDENTIAL information in accordance with the French security measures for protecting SECRET information.

Note 4 France: France does not use the classification ‘RESTREINT’ in its national system. France handles and protects RESTREINT UE/EU RESTRICTED information in a manner no less stringent than the standards and procedures described in the security rules of the Council of the European Union. France will handle classified information bearing the national classification markings of RESTRICTED level in accordance with its national rules and regulations in force for ‘DIFFUSION RESTREINTE’. The other Participants will handle and protect information marked ‘DIFFUSION RESTREINTE’ according to their national laws and regulations in force for the level RESTRICTED or equivalent, and according to the standards defined in the present document.

Note 5 Germany: VS = Verschlusssache.

Note 6 Portugal and Spain: Attention is drawn to the fact that the markings RESERVADO used by Portugal and Spain refer to different classifications.