



EUROPEAN
COMMISSION

Brussels, 25.5.2022
C(2022) 3403 final

ANNEX 3

ANNEX

to the

Commission Implementing Decision

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

ANNEX 3

2022 call topics description

Table of contents

1.	Content of the document	3
2.	Call topics description	4
2.1.	Call EDF-2022-RA	4
2.1.1.	EDF-2022-RA-MCBRN-HICP: Diagnostics, treatment, transport and monitoring of highly contagious, injured and/or contaminated personnel	4
2.1.2.	EDF-2022-RA-C4ISR-AIRC2: Single European Sky interoperability	8
2.1.3.	EDF-2022-RA-SENS-CSENS: Covert sensing	13
2.1.4.	EDF-2022-RA-SENS-ART: Advanced radar technologies	18
2.1.5.	EDF-2022-RA-CYBER-CSACE: Adapting cyber situational awareness for evolving computing environments	23
2.1.6.	EDF-2022-RA-SPACE-RSS: Responsive space system.....	27
2.1.7.	EDF-2022-RA-DIGIT-DBIR: Shared databases and integrated systems for image recognition	31
2.1.8.	EDF-2022-RA-ENERENV-CUW: Sustainable components for underwater applications	35
2.1.9.	EDF-2022-RA-MATCOMP-PACOMP: Packaging technologies for critical defence components	39
2.1.10.	EDF-2022-RA-PROTMOB-FMTC: Future mid-size tactical cargo aircraft	44
2.1.11.	EDF-2022-RA-UWW-UTS: Underwater manned-unmanned teaming and swarms.....	48
2.1.12.	EDF-2022-RA-UWW-ODAC: Underwater observation, detection, acquisition and communications	53
2.2.	Call EDF-2022-LS-RA-DIS.....	57
2.2.1.	EDF-2022-LS-RA-DIS-AC: Innovative technologies for adaptive camouflage.....	57
2.2.2.	EDF-2022-LS-RA-DIS-EAD: Electromagnetic artillery demonstrator	64
2.2.3.	EDF-2022-LS-RA-DIS-NT: Non-thematic research actions targeting disruptive technologies for defence	69
2.3.	Call EDF-2022-LS-RA-CHALLENGE	71
2.3.1.	EDF-2022-LS-RA-CHALLENGE-DIGIT-HTDP: Unmanned ground and aerial systems for hidden threats detection – Participation to a technological challenge	71
2.3.2.	EDF-2022-LS-RA-CHALLENGE-DIGIT-HTDO: Unmanned ground and aerial systems for hidden threats detection – Organisation of a technological challenge	75
2.4.	Call EDF-2022-DA	77
2.4.1.	EDF-2022-DA-C4ISR-EC2: European command and control system	78
2.4.2.	EDF-2022-DA-C4ISR-SOFC2: Deployable special operations forces multi-environment command post and C2 System.....	84
2.4.3.	EDF-2022-DA-CYBER-CIWT: Cyber and information warfare toolbox	88
2.4.4.	EDF-2022-DA-CYBER-CSIR: Cybersecurity and systems for improved resilience	92
2.4.5.	EDF-2022-DA-SPACE-ISR: Innovative multi-sensor space-based Earth observation capabilities towards persistent and reactive ISR.....	97
2.4.6.	EDF-2022-DA-SPACE-SBMEW: Space-based missile early warning	103
2.4.7.	EDF-2022-DA-MATCOMP-SMT: Smart and multifunctional textiles.....	107
2.4.8.	EDF-2022-DA-AIR-AEW: Airborne electronic warfare	113
2.4.9.	EDF-2022-DA-GROUND-CGC: Collaborative combat for land forces	118

2.4.10. EDF-2022-DA-NAVAL-MSAS: Medium-size semi-autonomous surface vessel	125
2.4.11. EDF-2022-DA-NAVAL-NCS: Naval Collaborative Surveillance	132
2.4.12. EDF-2022-DA-SIMTRAIN-MSSI: Modelling, simulation and simulator integration contributing to decision-making and training	138
2.5. Call EDF-2022-FPA.....	145
2.5.1. EDF-2022-FPA-MCBRN-MCM: Framework partnership agreement to support EU defence medical countermeasures Alliance	145
2.6. EDF-2022-LS-RA-SMERO	152
2.6.1. EDF-2022-LS-RA-SMERO-NT: Non-thematic research actions by SMEs and research organisations ...	152
2.7. EDF-2022-LS-DA-SME	154
2.7.1. EDF-2022-LS-DA-SME-NT: Non-thematic development actions by SMEs	154
2.8. EDF-2022-CSA-NFP	156

1. Content of the document

This document contains the description of all topics to be addressed by the eight EDF 2022 calls for proposals.

2. Call topics description

2.1. Call EDF-2022-RA

- **Targeted type of actions:** research actions.
- **Form of funding:** actual costs grants following the call for proposals.
- **Targeted type of applicants:** any eligible consortium as defined in Articles 9 and 10(4) of the EDF Regulation.
- **Indicative budget for the call:** the Union is considering a contribution of up to EUR 270 000 000 to support the following 12 call topics:

2.1.1. EDF-2022-RA-MCBRN-HICP: Diagnostics, treatment, transport and monitoring of highly contagious, injured and/or contaminated personnel

- **Indicative budget:** the Union is considering a contribution of up to EUR 25 000 000 for this topic under the call EDF-2022-RA.
- **Number of actions to be funded:** up to one action may be funded for this topic.

Objectives

General objective

Research and development in detection, diagnostics, treatment, transport and monitoring of highly contagious, injured and/or contaminated personnel (HICP) provides for new life-saving techniques, concepts and strategies for soldiers on the battlefield, including surgical robots, ultra-portable telemedicine devices and diagnostics sensors, Chemical Biological, Radiological and Nuclear (CBRN) containment systems, ‘porter’ or load- carrying Unmanned Vehicles (UVs) and battlefield casualty extraction devices. Battlefield logistics are a challenge regardless of the mission. Adversaries, terrain, and the environment all serve to complicate the process of delivering supplies to the wounded and sick. The medical support to a force must be capable of maintaining the necessary quality and quantity of supply, treatment and evacuation activities during peace, crisis, and conflict. This requires having on hand or in reserve appropriate medical equipment, supplies, integrated medical evacuation capabilities and remote casualty care capacity, as well as having the ability to resupply and to replace medical personnel on a continuous basis.

Specific objective

The limited ability to rescue HICP, while under fire or into a hazardous environment, is itself a major cause of poor outcome and death.

In the CBRN contaminated battlefield, combat-related injuries are “combined” – related to both, trauma and contamination. The time to aid a victim is crucial. This is even true for combination injuries. Hence there is a need to provide solutions for autonomous battlefield triage, safely extraction of HICP from the battlefield, providing instant availability information about vital signs, rapidly diagnosing life-threatening injuries, remote access of medical personnel to the casualty and delivering life-saving interventions. Extraction robots and dedicated evacuation vehicles may decrease the risk to the soldier and combat medic by life-saving robotic-assisted interventions, and by safely moving wounded soldiers out of the

line of fire. Tele operated and autonomous surgical robots may deliver expert surgical care within the “golden hour” on the battlefield as well as during transport to military treatment facilities. In CBRN situations, notably under radiation exposure, further restrictions have to be dealt with such as limited accessibility of the affected areas and concerns regarding the safety of the rescuing personnel.

Scope and types of activities

Scope

Proposals must address extraction, treatment, and evacuation systems, including detection, diagnostics, integrated life-support systems and transport of HICP. Proposals must in particular address:

- design of a dedicated CBRN casualty extraction device and/or adaptation and integration of existing capabilities, ‘porter’ or load- carrying UV/RGP¹ capable to locate, lift (scoop) and rescue, operating in hazardous and uneven/rough conditions,
- patient on-board life support and containment system supported by automated recording of vital signs to perform preliminary diagnostics and movement of casualties, containing ventilator, defibrillator, in-/out protection, and devices to monitor the physiological status of the patient to perform preliminary diagnostics,
- decontamination technologies for safe treatment and/or transport of HICP,
- robotics-assisted life-saving intervention, such as automated administration of anti-dots and/or haemostats or tourniquets,
- solutions for quick location of casualties and initial diagnosis, including triage, in case of CBRN events, for example based on wearable (bio)sensors or other sensor solutions.

In addition, proposals should also address:

- methods and concepts for seamless interoperability and complementarity of CBRN casualty extraction devices, whereas casualties could be evacuated by unmanned vehicles and robotic platforms and transported to medical treatment facilities,
- compatibility between transport types with plug & transport solutions leading to an enhanced responsiveness and resilience. E.g., by a modular platform system as a basis for multiple (unmanned) aerial or ground vehicles: (roll-on / roll-off platform system),
- integration of CBRN casualty extraction devices into health monitoring platforms and/or CBRN DIM² systems,
- harmonization of the different concepts of operation (interoperability) fostering the collaboration of EU Member States and associated countries with a standardized solution,

¹ Unmanned vehicle/Robotic ground platform

² Detection, identification, monitoring

- investigation of new possibilities to transport and assist HICP,
- semi-autonomous or ‘supervised’ surgical capabilities, concepts for material, structure design, ventilation and medical supply logistics for the safe transport and assistance (including treatment) of contaminated or contagious casualties in CBRN hazard area,
- evaluate the designated materials, the components and the final system during transport and assistance of contaminated/contagious casualties,
- selection of material and components, and evaluation according to suitable simulation and testing procedures.

Types of activities

The following types of activities are eligible for this topic:

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)	Yes (optional)
(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 design has been developed, including partial tests for risk reduction in an industrial or representative environment	Yes (mandatory)
(e)	System prototyping of a defence product, tangible or intangible component or technology	No
(f)	Testing of a defence product, tangible or intangible component or technology	No
(g)	Qualification of a defence product, tangible or intangible component or technology	No
(h)	Certification of a defence product, tangible or intangible component or technology	No
(i)	Development of technologies or assets increasing efficiency across the life cycle of defence products and technologies	No

The proposals must substantiate synergies and complementarity with foreseen, ongoing or completed activities in the field of MEDEVAC³ and RSS⁴, notably those performed or foreseen in the context of EDIDP, EDF 2021, Horizon 2020 and Horizon Europe.

Functional requirements

The proposed activities should address technologies to provide the following functional requirements:

- adaptable UxV evacuation vehicle and/or platforms for different operations (for example short/medium/long range transport of HCIP);
- air filtration system with air quality monitoring capability to be applied during transport, which would be adaptable for different CBRN conditions – HICP with different agents;
- option for transport of casualty/patient required ICU⁵;
- integrated decontamination system/capabilities;
- operate in extreme environments (including hazardous environments) and provide combat casualty care as close as possible to the point and time of injury;
- robust, light and small as possible, resisting fog, mud or dust and extreme temperatures, in order to assure a correct service in hostile environments and over debris surfaces;
- track, record, transmit and act upon continuous near-real-time measurement of physiological/health data rendered by wearable biosensors;
- locate and evacuate HICP from the battlefield using UxV evacuation platforms;
- carry / integrate a payload of medical supplies including a life support and surgical system capable to perform automated and/or robotic assisted lifesaving interventions, e.g., administer CBRN medical countermeasures using a robotic arm;
- (semi-) autonomous deployable surgical platform, including miniaturized surgical devices for robotic surgery to fit in casualty extraction UxV;
- integration of diagnostic, imaging and therapeutic capabilities (e.g., digital x-ray, portable ultrasound, intubation);
- smart textile sensor integration and wearable biosensors;
- carry / integrate into CBRN DIM system to provide early information as to the possible toxic hazards in the environment;

³ Medical evacuation

⁴ Reconnaissance and surveillance services

⁵ Intensive care unit

- remote assistance, including tele-medicine, such as technologies to communicate with a reach-back human medical team, imaging technologies and/or augmented reality technologies;
- protect the HICP during transport;
- for design of platforms, a manual with all tested and evaluated procedures should be prepared.

Expected impact

- Provide substantial improvements to the CBRN / medical defence domain for Member States and Norway armed forces that can revolutionize battlefield care by safely extracting casualties and patients from harm's way, rapidly diagnosing life-threatening injuries, delivering life-saving interventions and ensuring their safe transport (short-medium or long range) to dedicated medical facilities;
- Facilitate the development of CBRN / medical defence capabilities that each Member State, associated country, individual government or industry cannot face alone;
- Strengthen European sovereignty and contribute to the EU strategic autonomy;
- Develop EU autonomous industrial segments.

2.1.2. EDF-2022-RA-C4ISR-AIRC2: Single European Sky interoperability

- **Indicative budget:** the Union is considering a contribution of up to EUR 20 000 000 for this topic under the call EDF-2022-RA.
- **Number of actions to be funded:** up to one action may be funded for this topic

Objectives

General objective

In order to cope with sustained air traffic growth and operations over Europe, the Single European Sky (SES) initiative has been running since 2004. It intends to improve the performance of Air Traffic Management (ATM) in terms of safety, capacity, cost-efficiency and the environment. It hence paves the way for a European airspace that is used optimally, embraces emerging disruptive technologies, facilitates the integration of “new entrants” such as all types of drones, High Altitude Platform Systems (HAPS) to super- and hyper-sonic aircraft, trans-atmospheric and suborbital vehicles, and complies with emerging challenges. This modernisation of the civil aviation sector does not directly apply to military operations and training. However, civil and military aviation activities are closely interlinked, as they share the same airspace considered as a continuum. Therefore, SES implies a necessary coordinated modernisation of the different Air Command and Control (C2) systems, which are furthermore to collaborate at national and EU levels. Indeed, in this context, concomitant with a more hostile security environment, the timely sharing of correct and consistent information covering all phases of flight, between civil and military parties is a must.

Specific objective

The evolving SES regulations based on the harmonisation of the coordination and interoperability operational concepts or technical standards introduces in front of the military ATM stakeholder several new challenges which might be converted in opportunities for a more complete, optimized and performant Air C2 missions.

The introduction of the 4D Trajectory based management of the Air traffic and the new technical standards on the harmonisation of automatic ATM data exchanges need to be implemented in the Air C2 centres and systems.

The latest version of the European ATM Master Plan demonstrates the necessity to transform the ATM architecture due to several observed concerns that will have to be improved and optimised. These concerns are mainly the following ones:

- a steady increase of conventional traffic since 2014, even if the current sanitary crisis has drastically reduced the traffic, it is most probably a temporary situation;
- the growing environmental concerns raised by the aviation sector to demonstrate its capacity to contribute to the EU's environmental objectives;
- the appearance of new entrants into the airspace with the expected large number and heterogeneous nature of drones together with the emerging interest for operating vehicles at very high altitudes;

Against this background, Member States and Norway must be prepared from a military perspective to:

- Safeguard the military ambition to be trained for and to execute missions as required and more specifically to continue performing Air Surveillance and Control in the changing context of civil aviation sector (digitalization, automation, dynamic airspace management, new data format, resilience and cybersecurity issues), facing the density and diversity increase of air traffic,
- Ensure the interoperability and data exchange between civil and military control centres, including data sharing between classified and non-classified environment, permitting an efficient, secured and safe ATC⁶ (e.g., for military airports providing Air Traffic Services for civilian flights) and to support the planning, tasking and execution of air operations 24/7.

Scope and types of activities

Scope

Military airspace users' main challenges are to continue to provide, and further improve, defence and security missions, with needs of high degree of flexibility and reactivity, into an airspace shared with civil airspace users, without prejudice to the safety of civil air traffic, and considering, to the maximum extent possible, the performance and environmental objectives of the civil aviation sector.

In order to do so, the scope of the activity consists in increasing interoperability of military Air C2 systems against SES rules via an interoperability demonstration. The activity must

⁶ Air traffic control

focus on identifying technical solutions for information and data exchanges between cross border military C2 systems and cooperating civil – military ATC systems based on new challenges generated by the evolution of the SES harmonisation deployment regulation and new possibilities offered by information technologies.

In particular, the implementation and assessment of new rules of Interoperability (IOP) for surveillance and control of the European air traffic from a military perspective are the main objectives of this call. Several technical standards must be implemented, and solutions developed to ensure the harmonized, efficient and secure data exchanges between relevant civil and military stakeholders:

- Technical interoperability for real time flight and airspace management data exchanges (with relation to ability to exchange, exploit and fill Flight Objects, etc.);
- Security aspects to ensure cross-domain exchanges (with regards to secure gateway or procedures to limit dissemination of sensitive military information, facilitating sharing of military information to enhance civil situational awareness, etc.);
- Assessment of resulting ATM safety levels as any ATC civil-military interoperability system.

Types of activities

The following types of activities are eligible for this topic:

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)	Yes (optional)
(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 design has been developed, including partial tests for risk reduction in an industrial or representative environment	Yes (mandatory)
(e)	System prototyping of a defence product, tangible or intangible component or technology	No
(f)	Testing of a defence product, tangible or intangible component or technology	No

Types of activities (art 10(3) EDF Regulation)		Eligible?
(g)	Qualification of a defence product, tangible or intangible component or technology	No
(h)	Certification of a defence product, tangible or intangible component or technology	No
(i)	Development of technologies or assets increasing efficiency across the life cycle of defence products and technologies	No

The proposals must substantiate synergies and complementarity with SES, including SESAR, activities.

Functional requirements

The technical solutions for information and data exchanges between cross border military C2 systems and cooperating civil – military ATC systems should meet the following functional requirements:

(1) Situational Awareness establishment and exploitation

- Improve surveillance and flight identification data capacity
- Improve situational awareness and operational flexibility
- Identify better conditions to accommodate the mission-specific requirements derived from the introduction of new generations of military manned and unmanned aircraft and systems.

(2) Coordination and IOP assessment

- Improve flight information automatic exchange for coordination purposes
- Facilitate hand-over of aircraft control
- Identify and develop a military solution of common interest for European forces and compliant with SES regulation for the ATM civil-military, and military-military exchanges
- Integrate data compliant with SES technical standards used for IOP exchange between civil-military ATC systems or military Air C2 systems of cross-border countries
- Implement Operational Air Traffic (OAT)/General Air Traffic (GAT) rules.

(3) Cross-domain connectivity establishment and services provision

- Assess the impact of the new pan-European network service (NewPENS) and the system-wide information management (SWIM) service-oriented architecture, including SWIM Nodes (for military operation system) access procedure, based on available standard interfaces to the military infrastructure and services delivery architecture (SWIM Blue for the interoperability)

- Identify the level of performance/quality of service requirements as the basis to select the applicable SWIM-TI (technical infrastructure) profile
- Develop interfacing and IP (internet protocol) networking approaches supporting SWIM-TI accessibility
- Comply with NewPENS and SWIM services, including related standardization rules
- Identify proprietary/local interoperability options outside the context of SWIM to ensure service continuity and redundancy and diversity of connections for military systems
- Design and develop an evolving, scalable cross-domain solution supporting the information exchanges between ATM civil-military and military-military centres
- Validate end-to-end information exchanges via the SWIM TI, between ATM military centres from European forces and between ATM civil and military centres in accordance with the regulation of the SES and national security rules.

Expected impact

This collective work should provide individual and mutual benefits, for European Member States, Norway and the industry, in different fields as follows:

- European Technology
 - Reinforcement and security improvement of data exchange between cross domain (classified and unclassified environments)
 - Improvement of air surveillance performances and flight's safety
 - Improvement of Dynamic Airspace Management
 - Capitalisation of on field proven Research & Development (R&D) process and ensure limited in time project
 - Production of consolidated R&D data for further industrialization phase
- European Autonomy
 - Contribution to the enhancement of sensible data sharing between ATM stakeholders
 - Maintenance and enhancement of autonomous control of the European defence capabilities
 - Protection of the environment of the European citizen
- European Security
 - Participation to the improvement of the airspace surveillance and control, and air policing missions

- Facilitation of military forces projection and intervention
- Enhancement of cooperation between Member States and Norway for defence matters.

2.1.3. EDF-2022-RA-SENS-CSENS: Covert sensing

- **Indicative budget:** the Union is considering a contribution of up to EUR 25 000 000 for this topic under the call EDF-2022-RA.
- **Number of actions to be funded:** several actions, addressing different solutions, may be funded for this topic

Objectives

Due to the current geopolitical instability, European military forces will be obliged to participate in demanding military multi – domain operations like securing air superiority, land and sea control, border surveillance, traffic management, security of critical infrastructures, etc. Military information superiority is key to these operations, because they are relying on the best possible battlefield awareness, which is created by the exploitation of data acquired by modern sensors, integrated both in a range of platform and in a range of concepts of use enabled by the digital transformation of the battlefield.

General objective

Given the sensors' technological progress, the European military forces may encounter potential adversaries capable of obtaining a robust situational awareness by using advanced active and passive sensor capabilities, able to accurately locate and identify forces and their sensors in the three-dimensional battlespace (land, sea and air). For efficient Intelligence, Surveillance, Target Acquisition and Reconnaissance (ISTAR) missions, armed forces therefore need to have sensors that reliably allow detection, classification and tracking of targets while being themselves difficult to detect, track and intercept. The capability to sense covertly allows unhindered operation without exposing location and identity to the enemy surveillance activities, thus lowering the vulnerability of own forces and conferring a key advantage in military conflicts.

In the modern operational environment, there are targets with properties resulting in low probability of detection, due to their low signature or manoeuvring characteristics (very fast or very slow, up to hovering). Targets can also be difficult to detect due to the operation conditions (such as in urban scenarios, under foliage, underground or underwater operation or operating at low altitude) leading to strong clutter or a degraded visual environment. Recent advances in computing power, digital data and signal processing, together with the drastic reduction of size, weight and overall dimensions of equipment due to the advancement of microelectronics technology, have paved the way for better sensors, with increased sensitivity and better detection characteristics.

Examples of use-cases, where covert sensing of difficult targets is of particular importance include:

- counter-battery fire;
- detection of sea surface targets (drones, periscopes, wooden boats, communication buoys...);

- air defence and detection, recognition, identification and tracking of aerial targets (including low flying, slow, small drones);
- detection of fast manoeuvring and fast-moving targets with up to hypersonic speeds, like tactical ballistic missiles and anti-ship missiles;

Specific objective

Modern surveillance sensors have to comply with operational requirements such as:

- To provide steady and reliable surveillance (detection, tracking, classification, identification), at various environmental conditions – for all battlespace dimensions, with guaranteed low probability of false alarms
- To detect and track targets that are difficult to detect in complex environments, like rural, coastal and mountainous areas with complex relief, semi-urban and urban environments, etc.
- To operate covertly, exhibiting low (for passive sensors) or reduced (for active sensors) signature to enemy counter- intelligence, surveillance and reconnaissance (ISR) assets, thus reducing the possibility of being intercepted and countered,
- To be capable of supporting target acquisition in all mission phases and to support target engagement on the move, in particular by continuing interpretation and processing of data while the sensor and / or the target are moving or changing position.
- To have improve sustainability under harsh operational conditions in full battlespace dimensions (sea, air and land)
- To provide robustness in contested environments, with scenarios that are becoming more and more dynamic with highly agile targets.
- To be able to be integrated in various types of static and moving platforms (ground-based, shipborne, airborne, space-based), both manned and unmanned;

Covert sensing concepts can in principle include:

- Passive sensors that are less traceable and are hard to target and
- Active sensors with very low probability of intercept, in particular when used in specific configuration (multi-static configurations...)

Such sensors can be based on different types of physical phenomena (to detect different electromagnetic wavelength, acoustic waves, photons...) and on different working principle.

To use the advantage of a multi-sensor and multi-spectral approach, the sensors may need to be integrated into a network of multiple heterogeneous sensors and provide data that can be merged with data from other sources.

Scope and types of activities

Scope

This topic aims at enhancing detection performance (such as range, sensitivity, resolution) of sensor systems to detect low signature targets, in the modern three-dimensional operational environment while maintaining covert operation, without exposing presence, identity and location. It encompasses innovative concepts of sensor use, in particular the combination of multiple, heterogeneous sensors, potentially on different platforms.

Considered sensors may be electro-optical/infrared, radiofrequency and/or acoustic sensors, not excluding innovative sensor concepts. They must be passive or low-observable active. The topic covers the enhancement of individual sensors as well as their interplay.

The sensors' integration and interoperability with other sensors (networks) and connection to battlefield management systems must be addressed, e.g., through standardized data formats and interfaces or data processing (up to data fusion) on the sensor level.

Proposals should address the optimization of available sensor resources in order to achieve optimum surveillance results. Proposals should also address aspects of efficient data exploitation and data fusion close to the data source.

Types of activities

The following types of activities are eligible for this topic:

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)	Yes (optional)
(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 design has been developed, including partial tests for risk reduction in an industrial or representative environment	Yes (mandatory)
(e)	System prototyping of a defence product, tangible or intangible component or technology	No
(f)	Testing of a defence product, tangible or intangible component or technology	No

Types of activities (art 10(3) EDF Regulation)		Eligible?
(g)	Qualification of a defence product, tangible or intangible component or technology	No
(h)	Certification of a defence product, tangible or intangible component or technology	No
(i)	Development of technologies or assets increasing efficiency across the life cycle of defence products and technologies	No

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

- Generating knowledge:
 - o Research on low-signature active sensors as well as very high sensitivity passive sensors
 - o Activities aiming at improving the ability of sensors to operate in difficult conditions
- Integrating knowledge:
 - o Activities aiming at improving communication and connection between sensors

Among other tasks that the applicants deem necessary, the following tasks must be performed as part of the mandatory activities of the project:

- Studies
 - o Definition of relevant targets and operational conditions
 - o Definition of performance evaluation techniques and parameters for detection and classification solutions.
 - o Study and modelling of relevant signatures of targets and of complex environments, e.g., rural, coastal and mountainous areas with complex reliefs, semi-urban and urban environments, etc., and under different weather conditions.
 - o Study on enhancing performance robustness when dealing with different platform dynamics, stability, and manoeuvring conditions, different targets and environments.
 - o Study of data fusion techniques for improving detection and classification performances in different sensors configurations
 - o Study on interfaces and data exchange formats to provide efficient data fusion and exploitation, taking into account standards used by the EU Member States and Norway armed forces.
- Design

- Design of a system of passive or low-observable active sensors to detect targets of interest
- Demonstration of the performance of the system in a simulated environment, if possible, including real data where relevant to improve modelling and demonstration
- Demonstration of the performance of the system in a laboratory environment

Functional requirements

Proposals should address technologies and solutions that:

- significantly increase detection performance with respect to new and challenging targets in harsh operational environment;
- significantly increase performance robustness against changes of the environment and the target characteristics;
- Are adaptable to different and complex scenarios (e.g., electromagnetically congested, dynamic, with degraded visibility and rapidly changing), enabling multi-mission and multi-platform applications (maritime, land and air);
- have reduced size, weight and power consumption, for scalable integration on differently sized manned or unmanned platforms;
- Are compatible with modular and scalable architectures;
- Are compatible with multi-sensor and multi-spectral approaches;
- Ensure interoperability with other systems by providing standardized interfaces and data exchange formats used by the EU Member States and Norway armed forces;
- simulate and automatically configure sensor configurations to carry out data fusion while optimizing the available resources and achieving the optimum surveillance results;
- Allow efficient exploitation and data fusion from multiple static or deployed sensors;
- are capable of executing data processing and analytics close to the data source to decrease the capacity needs to transfer sensor data;

Expected impact

- New knowledge in the field of covert sensors, sensor systems and their interplay, thereby strengthening the European technological and industrial base.
- Future EU critical land, naval and air ISTAR capabilities in highly dynamic scenarios, especially regarding challenging targets, increasing situational awareness, early warning, decision making and action planning capabilities.
- State of the art, covert sensing capability that increases survivability of units/platforms
- Increase of interoperability and efficient use of sensor systems thereby facilitating joint operations among armed forces of the EU Member States and Norway.

2.1.4. EDF-2022-RA-SENS-ART: Advanced radar technologies

- **Indicative budget:** the Union is considering a contribution of up to EUR 15 000 000 for this topic under the call EDF-2022-RA.
- **Number of actions to be funded:** several actions, addressing different solutions, may be funded for this topic.

Objectives

General objective

Passive and active radio-frequency (RF) systems in general and surveillance radar systems in particular remain vital assets for supporting multi-domain operations: incl. air and air defence missions, as well as ground/maritime operations.

Management of the electromagnetic spectrum has increased in importance. Radar operation must be compatible with other communication and control systems running concurrently. Management of emission and sensing in both space and frequency increases the systems covertness. It also improves the system's ability to discriminate reliably signals coming from passive and civilian sources as well as active disturbances such as jammers and decoys.

Emerging technologies lead to the increased appearance of threats that are difficult to detect and track due to their low radar cross-section (RCS) (e.g., stealth technologies), manoeuvring characteristics (e.g., hypersonic weapon systems, slow-moving airborne units) or saturation attack tactics. Facing such a wide spectrum of threats (in terms of variation of speed, angle of approach and altitude), existing surveillance systems are reaching their limits in terms of detection range, angular domain coverage, and tracking capabilities. Specific operating modes (e.g., multistatic configurations) can improve detection and tracking performance. They however lead to an increased requirement on multiple beams forming. Proper detection, recognition and classification of different targets in a variety of operational conditions also requires a finely tuneable band.

Specific objective

Those operational and technical challenges can be met by future systems with:

- agile digital beamforming to optimise observation time, volume coverage and detection reliability
- System characteristics such as wide or ultra-wide band coverage, low noise, high coherence
- Software defined waveforms with high degree of flexibility and use of multiple bands
- Data processing functions to enhance detection performance, target recognition and classification, notably with respect to new threats

In order to be operated in various conditions and to be integrated in various platform, specific requirements moreover apply to the dimensions, weight and energy consumption of the radar modules (e.g., through miniaturization or grouping of functions in small electronic units) as well as their materials and electronics design to ensure optimal operability in harsh conditions. Efforts are also aiming at integrating multiple functions (radar, communication, electronic warfare) in a single radio frequency system for multi-role systems (e.g., see call PADR-EMS-03-2019).

Scope and types of activities

Scope

Recent research and development efforts in the field of radar and electronic warfare systems have the goal to create more flexible and adaptive systems in terms of modes of operation and beamforming. At the same time, new technologies offer possibilities to explore different frequency (or bandwidth) ranges while maintaining a high signal-to-noise ratio. A further objective is to integrate more functions, including internal computing capacities, while responding to the operational restrictions in terms of size, weight and power consumption and cost (SWaP-C).

The scope of this call topic focusses on electronic components and their integration that help to accomplish the above-mentioned goals by achieving:

- improved size/weight/power ratios through miniaturisation and system integration
- Integration of new technologies to increase the system's adaptability to environments and operational scenarios.
- Demonstration of agile and precise radar beam steering and detection performance.

The following enabling technologies serve as examples for the improvement and integration scope of this topic, without excluding other relevant technologies:

- direct sampling technologies able to perform data conversion in any radar frequency band, reducing the RF front-end complexity and maximizing the miniaturisation;
- hardware and software components for digital beamforming, including using photonic components, that enable generic and reconfigurable digital beamforming, especially with true-time delay, broadband characteristics, multi-beam capability;
- Hardware and software that would allow real time signal and data processing coming from digitized received signals at radiating element level in order to extract and store the information on targets including detection, tracking and classification;
- Components that enable the generation of extremely stable radio-frequency signals
- Antenna components that emit in a broad frequency band with low spurious emissions to adapt to the environment, e.g., by exploring fully polarimetric active electronically scanned array (AESA) antennas which are more robust against interferences and can enable enhanced performance in terms of detection and classification.

Proposals should target a substantial technological advancement in order to bring the considered components to a maturity level corresponding to laboratory testing or higher (technology readiness level TRL > 4).

Furthermore, proposals may include complementary aspects on:

- application of artificial intelligence as a means of enhancing target detection, classification and identification performance, notably with regards to new threats, including to enable cognitive radar concepts.

- Integration aspects (such as interfaces with other sub-subsystems and data exchange formats) including high data rate transfer to other sub-systems (software and/or hardware aspects), in particular enabling distributed radar setup and Command and Control integration

This topic complements past and ongoing research and technology efforts supported by the EU, e.g., through the calls PADR-EMS-03-2019, PADR-EDT-02-2018 and the calls EDF-2021-SENS-R-RADAR, EDF-2021-MATCOMP-R-RF as well as Member States' and Norway's efforts, including in the EDA framework.

Types of activities

The following types of activities are eligible for this topic:

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)	Yes (mandatory)
(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 (mandatory)
(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 design has been developed, including partial tests for risk reduction in an industrial or representative environment	Yes (mandatory)
(e)	System prototyping of a defence product, tangible or intangible component or technology	No
(f)	Testing of a defence product, tangible or intangible component or technology	No
(g)	Qualification of a defence product, tangible or intangible component or technology	No
(h)	Certification of a defence product, tangible or intangible component or technology	No
(i)	Development of technologies or assets increasing efficiency across the life cycle of defence products and technologies	No

Among other tasks that the applicants deem necessary, the following tasks must be performed as part of the mandatory activities of the project:

- Generating knowledge:
 - Research on software and hardware solutions for processing digital signals collected after RF direct sampling for sensors
 - Investigation of technologies and components for wideband or multiband direct sampling
 - Exploration of innovative antenna design
 - Investigate cognitive approaches that enables adaptability of the system to the environment and the scenario.
 - Investigation of technologies and components for ultra-low phase noise oscillators
 - Investigation of improvement of SWaP-C for the considered components.

The proposal may also address optionally the following tasks under this activity:

- Prepare suitable model of targets, threats and environment for training artificial intelligence (AI) -based algorithms;
- Integrating knowledge:
 - Explore scenarios and algorithms to improve the performance in scenarios including low RCS targets and highly manoeuvring targets such as hypersonic ones.
 - Explore the applicability or adoption of components and technologies from civil applications to defence designs

The proposal should moreover address the following tasks under this activity:

- Investigation of solutions, such as algorithms, to increase system resilience against Cyber Electro Magnetic Activities (CEMA) and similar threats
- Investigate “secure by design” technologies that can be used to increase system resilience in case of cyber-attacks;
- Studies
 - Selection of relevant operational scenarios
 - Exploitation of numerical simulations, e.g., based on digital twins, for testing new hardware and software solutions
 - Study of advanced antenna architectures, including innovative thermal management solutions and material, reducing size, weight and power consumption (acceptable SWaP for airborne applications) while providing enhanced surveillance and tracking capabilities;

The proposal may address the following tasks under this activity:

- Study on technology for sharing and distributing classified data from RF sensor systems;

- Study on the use of AI techniques for system design and concept
- Design
 - Design of digital beamforming and testing in a laboratory environment
 - Design on-board computing solutions for deployment of signal and data processing algorithms enabling enhanced and real-time computing capabilities and demonstration of performance in a laboratory environment;
 - Design of digital twins for testing of new hardware and software solutions and demonstration in a laboratory environment;
 - Design of advanced antenna architectures, including innovative thermal management solutions and material, reducing size, weight and power consumption (acceptable SWaP for airborne applications) and demonstration in a laboratory environment;
 - Validation of the adaptive capabilities of the system by tests in a simulated environment and in a controlled environment.

Functional requirements

Proposals should address technologies and solutions that

- Integrating wide bandwidth components and building blocks for achieving better detection, tracking and, classification performances of radio-frequency sensor systems, including for challenging threats;
- Enabling versatility and reconfigurability with respect to system functions and operational modes (e.g., tracking modes, imaging modes, beam modes, waveforms)
- Enabling adaptability to the scenario and the operational conditions
- Supporting innovative antenna design (e.g., ubiquitous approach decoupling the observed area from the physical antenna position, conformal arrays)
- Enabling operation in multi-static radio-frequency system architectures, especially taking into account synchronisation issues;
- Capable of coping with increased data rate and volume with respect to signal acquisition and data processing
- Demonstrating modular and scalable architecture with suitable weight, size and power consumption (SWaP) to be implemented over a variety of platforms (including airborne applications as well as unmanned vehicles)
- Ensuring compatibility with simultaneously operated civil systems (including telecommunication applications) and defence systems;
- Ensuring interoperable interfaces and data formats with other military and civil sensor systems.

Expected impact

- Contribution to the capacity and the technological autonomy of technological and industrial actors in the EU Member States and Norway to develop new radio-frequency systems.
- Building capability to define, develop and operate radio-frequency systems for surveillance, detection, tracking and classification of objects that are difficult to detect and track in increasingly difficult environments and operating conditions.
- Increased flexibility of radio-frequency systems to create multifunctional, fully digital systems, able to adapt to the situation and the environment.
- Enhancement of the integration of radio-frequency systems in distributed control and surveillance platforms.

2.1.5. EDF-2022-RA-CYBER-CSACE: Adapting cyber situational awareness for evolving computing environments

- **Indicative budget:**

The Union is considering a contribution of up to EUR 10 000 000 for this topic under the call EDF-2022-RA

- **Number of actions to be funded:** Several actions, addressing different solutions, may be funded for this topic

Objectives

General objective

An increasing number of malicious actions targeting governmental and strategic systems occur in cyber space. New or improved solutions, technologies and applications for enhanced cyber situational awareness (CSA) are essential to counter these threats. To address evolving and more complicated activities in cyberspace, including challenges that arise due to the ongoing evolution of battlefield network and systems, decision makers and Security Operation Centre (SOC) operators need the most updated CSA related to cyber threats, in real time, gathering internal and external cyber information. CSA denotes the capability for a decision-maker to know what is going on in the cyber domain in order to be able to make informed decisions and adequately respond to incidents.

Specific objective

CSA needs to be supported by technology to collect, correlate and fuse the several sources of data as well as their different nature (e.g., network, mission, open-source intelligence, structured and unstructured threat awareness) to provide the necessary information so that human decision-makers can assimilate the situation. Cyber threats continue to grow in complexity and scope, new and evolving threats arising from advancing adversary campaigns and tactics and at the same time the volume and diversity of cyber threat intelligence grows all the time. It poses challenges to human operators to visualise and comprehend the variety and volumes of information produced by dynamic and fragmented networks and systems in a battlefield context. The evolving computing challenges will require improved mission awareness capabilities through Cyber Threat Intelligence (CTI) establishing interfaces with

sources of information considered relevant for the planning and conduct phases of an operation in order to provide real time mission information at the correct level of granularity to the common operational picture (COP).

Scope and types of activities

Scope

The overall goal is to explore novel concepts and operational opportunities for providing to the Commander essential intelligence about the adversary, their capabilities and objectives while operating in and through cyberspace. CTI enhanced with a Semantic Threat Enrichment module able to analyse both data coming from public repositories and the dark web to generate Indicators of Compromise (IoCs) and Indicators of Attacks (IoAs) will support Cyberspace Operations.

The proposals are expected to develop novel solutions leveraging full-spectrum cyber defence (physical, logical, cyber persona) under an adversarial-focused perspective. The proposals are expected to aim at CSA-supporting technology with a view to provide the necessary technical information elements that are needed to process the vast amounts of information in order to produce from tactical to COPs, as well as other technical artifacts to be used by decision-makers in need of CSA. This includes creation of graphics like timelines, histograms or relationship graphs, personalized dashboards, and reports according to the responsibilities of each user. Special attention shall be paid to the interoperability and collaboration with existing solutions at Security Operations Centre (SOC), Network Operations Centre (NOC) and Computer Emergency Response Team (CERT) level, where duplication of effort is to be avoided.

The proposals are expected to cover state of the art technologies. Enhanced situational awareness information handling and visualisation systems are expected to have a capability to present overarching views of the battlefield environment through COPs via data exportable modules of logic information to be interoperable with other operational pictures be at land, sea, air or space, taking into account ongoing evolution of the C2 military systems towards the Internet of the Military Things (IOMT) scenario which poses additional complexity, and sustain against a massive attack to critical battlefield system.

Types of activities

The following types of activities are eligible for this topic:

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)	Yes (optional)
(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	Yes (mandatory)

Types of activities (art 10(3) EDF Regulation)		Eligible?
	and solutions	
(d)	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, including partial tests for risk reduction in an industrial or representative environment	Yes (mandatory)
(e)	System prototyping of a defence product, tangible or intangible component or technology	No
(f)	Testing of a defence product, tangible or intangible component or technology	No
(g)	Qualification of a defence product, tangible or intangible component or technology	No
(h)	Certification of a defence product, tangible or intangible component or technology	No
(i)	Development of technologies or assets increasing efficiency across the life cycle of defence products and technologies	No

The proposals must include studies and design. The proposal may include generating knowledge and integrating knowledge activities.

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

1. Development of a number of typical user scenarios based on stakeholder needs. Entails analysis of battlefield IOMT technology requirement and their impact on the collection, correlation and presentation of information. It will include advances in terms of organisational, leadership and human training capability aspects. These will take into consideration human-machine interphases and performance optimisation in e.g., cyber SOCs.

2. The use of the digital twin concept and human factors analysis to improve operator information acquisition and processing through enhancing the current COP artefact technologies. Digital twins can allow to overcome operational technology (OT) constraints due to the need to be continuously operational and the fact they often provide only limited in-depth analysis capabilities. Digital twins can run in parallel to their physical counterparts and allow inspection of their behaviour without the risk of disrupting operational services.

3. Development of different hierarchical models to support IOMT mission awareness. These should establish means of aggregating dependency information to propagate only mission relevant, abstracted information rather than entire network configurations. Moreover, these systems must be able to exchange dependency information between and across federated IoT systems from different organisations/trust domains.

4. Design of an AI multi-stage (i.e., multi kill chain steps) attack detection architecture that maps AI-based anomaly detection models onto the distributed enterprise infrastructure. This will enable efficient temporal and spatial correlations of the event streams from different endpoints. This is expected to exceed the performance of conventional centralized security systems through improved detection of cross-network attacks and greatly reduced data communication. Moreover, it is essential to integrate threat modelling and sharing with attack detection to achieve efficient real-time detection using AI.

5. The use of federated learning to create a collaborative intrusion detection system (CIDS) to enhance the inter-domain sharing of mission-oriented CTI as well as remove many of the trust and privacy issues associated with CTI sharing. In this approach no actual alerts are shared, rather the AI model parameters are shared. This will ensure that there is no leakage of sensitive network, organisational or personal information. Moreover, the CIDS pattern can be implemented within a single organisation through judicious partitioning.

6. The use of digital ledger technologies to facilitate more dynamic and incentivised mission-oriented CTI sharing analysis between organisations well as increasing trust in sharing of intrusion model parameters between cross-domain federated learning entities will be investigated.

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

7. linking observed tactics and techniques to specific Advanced Persistent Threat (APT) behaviour, which may assist with adversary characterization and identification;
8. use of deception technologies, including decoys, both for monitoring the threat landscape and attackers' behaviour, and for intrusion detection. Particular attention should be on making the data from such systems can be presented in useful ways, and integrated with other sources of information;
9. use of machine learning technology.

The proposals must substantiate synergies and complementarity and avoiding unnecessary duplication with projects awarded under EDIDP calls for proposals.

Functional requirements

Proposals should meet the following functional requirements:

- Definition of a number of use-case scenarios to test the concept.
- Development of proof-of-concept implementations to verify the operation.
- Design of a cyber-range-based environment simulation to both generate representative data sets to validate the AI models and to provide a testbed to evaluate the overall concept.

Expected impact

The outcome is expected to contribute to:

- Better understanding of how CTI along with future technology will be able to support an analyst's build-up and conservation of a high level of CSA.
- Improved visualisation metaphors and information handling processes arising from IOMT scenarios.
- Improved CSA management through simulation capabilities provided by digital twins.
- Improved mission-to-asset awareness for IOMT supported mission infrastructures.
- Increased CTI sharing due to use of federated learning to prevent leakage or need to share sensitive information.
- Better understanding on the use of distributed anomaly detection in both single organisation constituencies as well as the effectiveness of collaborative intrusions on improving attack detection.

2.1.6. EDF-2022-RA-SPACE-RSS: Responsive space system

- **Indicative budget:** The Union is considering a contribution of up to EUR 20 000 000 for this topic under the call EDF-2022-RA
- **Number of actions to be funded:** Up to one action may be funded for this topic

Objectives

General objective

The general objective of this research topic is to pave the way towards a future European responsive space system able to place small satellites in various types of orbits within a short notice in order to address specific operational needs, including tactical ones, and capability gaps stemming from shortage, failures and damages of existing space assets. This is particularly relevant in the field of intelligence, surveillance and reconnaissance (ISR) and satellite communication (SATCOM) where space assets have to be continuously operational and available to monitor and react to risks and events.

Such a responsive space system will enhance the resilience and autonomy of the Member States, Norway and of the European Union in the fields of 'access to space' and 'space capabilities for defence applications.

Specific objective

The specific objective of this topic is to define the concept of operations (CONOPS) of such a responsive space system and to identify and compare suitable and affordable architectures and solutions for the end-to-end system. In order to be able to provide mission critical responsiveness in terms of reconstitution, replenishment or augmentation of space assets, the responsive solutions need to be considered within a broader space defence ecosystem. In this respect, the multiple logistical challenges required by an end-to-end system that needs to operate at a tactical pace should also be taken into account.

Scope and types of activities

Scope

Project proposals must address collaborative defence research on the CONOPS and architecture of a responsive space system composed of a launch infrastructure (including fixed sites and/or mobile carriers), launch vehicles and spacecraft (satellite platforms and payloads) concepts as well as the ground segments and stations needed to operate the launcher and the satellite/payload. Project proposals must consider various options for each component of the system based on existing solutions, adapted solutions and/or new developments. In particular, terrestrial, maritime or airborne launch solutions must be considered.

Types of activities

The following types of activities are eligible for this topic:

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)	Yes (optional)
(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 design has been developed, including partial tests for risk reduction in an industrial or representative environment	Yes (optional)
(e)	System prototyping of a defence product, tangible or intangible component or technology	No
(f)	Testing of a defence product, tangible or intangible component or technology	No
(g)	Qualification of a defence product, tangible or intangible component or technology	No
(h)	Certification of a defence product, tangible or intangible component or technology	No
(i)	Development of technologies or assets increasing efficiency across the life cycle of defence products and technologies	No

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

- consolidation of CONOPS from end-users, from user request for launch and preparation of the launch to ground and space segment interaction during launch and orbital phases;
- identification of main mission use cases for the responsive space system;
- preliminary analysis of the applicable regulatory framework (*e.g.*, compliance with NOTAM⁷/NOTMAR⁸ requirements, launch security and safety requirements including stage re-entry, mission abort...);
- definition of the overall conceptual architecture for the end-to-end system and associated high level requirements; the system must include the following subsystems:
 - o the launch infrastructure ensuring the purposes of launch preparation, launch pad and launch range (including fixed sites and/or mobile carriers);
 - o the launch vehicle (rocket);
 - o the spacecraft composed of satellite platforms and of a family of sensors dedicated to missions;
 - o ground segments for the launcher, the spacecraft, including fixed/mobile ground stations for space data reception and the necessary means of encryption;
- identification of high-level requirements for the launch infrastructure and of suitable launch zones to launch terrestrial, maritime or airborne systems on short notice:
 - o identification of suitable starting points (where the carrier departs) and launch areas (where the launch vehicle departs). Starting points must consider terrestrial, maritime or airborne mobile carriers;
 - o this must include an overview and comparison of all existing and new planned launch sites having assembly, integration and test (AIT) and storage facilities and possibility to host mobile carriers in the EU or associated countries with their individual pros and cons (*e.g.* vertical, horizontal, maritime launch and airborne launch concepts; safety and ecological implications; suitability for one or more launch providers; reachability by truck, airplane, train;; reachable orbits; security measures to handle defence systems);
 - o this task must consider phases from pre-flight to mission preparation and execution (including management of prepositioned payloads, propellant loading systems, *etc.*);
- identification of high-level requirements for the launch vehicle:

⁷ Notice to air missions.

⁸ Notice to mariners.

- including volume under fairing, standardization requirements (including fairing interface), propulsion type, injection precision and required deltaV, operational life expectancy;
- identification of high-level requirements for the spacecraft:
 - types and related performances (minimum standards);
 - standardisation, affordability and modularity/flexibility should be part of the analysis;
 - ability to be merged with the orbital upper stage should be looked at;
- identification of high-level requirements and definition for the ground segments and stations needed to operate the launcher and the satellite mission (platform and payload);
 - this task should include analysis of security requirements (encryption);
 - this task should also include a preliminary analysis of the sharing and booking mechanism for the system;
- identification and analysis of existing solutions able to meet the requirements and of needs for adaptations or for new research and development actions with their associated roadmap;
- costs vs benefits analysis (informed by CONOPS and architecture definitions) of the different options identified;
 - comparison of the proposed options in terms of costs / coverage of use cases and associated performances / safety constraints / logistics constraints / other implementation constraints / potential of evolution (*e.g.*, reachable orbits, increased mass...);
 - the analysis must take into account the lifecycle cost including launch infrastructure, launch vehicle, spacecraft (satellite platforms and payloads), ground segments, including all required ground facilities for prepositioned payloads, pre-flight operations including propellant loading, cryogenic (if needed) storage solutions, safety storage facilities for solid, hybrid or liquid propulsion, end-to-end maintenance, repair and operations;
 - the analysis must also take into account the logistical aspects and include preliminary technical and logistical trade-offs between propulsion solutions;
- preliminary requirements review (PRR) guided by the end-users (from Members States and Norway).

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

- simulation of the achievable responsiveness (end-to-end performances) of selected options for selected mission use cases / scenarios;
- preliminary design of selected sub-systems (to be proposed by the applicants).

Functional requirements

The responsive space system is expected to meet the following requirements:

- time between request for launch and positioning into orbit should be less than 72 hours including flight range safety measures. Time to operational data delivery can be shorter, depending on the precision of orbit injection, the type of orbital propulsion, the type of sensors and related calibration in space;
- ability to reach any low earth orbital plane, from equatorial to sun-synchronous polar orbits, while minimizing the operating and logistical constraints (operable from various types of areas);
- ability to place a satellite between 20 kg and 200 kg into an orbit of at least 400 km.

Expected impact

The action should produce the following expected impacts:

- set the basis for the development of a responsive space capability not yet available at European level;
- creation of a sovereign supply chain in Europe for defence capabilities in the domain of responsive space systems;
- leveraging the European defence technological and industrial base in the domains of launch infrastructure (including mobile carriers), rockets and satellite platforms and sensors;
- extension of EU launch solutions portfolio and strengthening of the EU autonomy in this field.

2.1.7. EDF-2022-RA-DIGIT-DBIR: Shared databases and integrated systems for image recognition

- **Indicative budget:**

The Union is considering a contribution of up to EUR 25 000 000 for this topic under the call EDF-2022-RA

- **Number of actions to be funded:** Several actions, addressing different solutions, may be funded for this topic

Objectives

Image recognition technologies become essential for defence applications. There is in particular an increasing need for forces to analyse their environment more efficiently in order to enhance decision-making, responsiveness and survivability while ensuring the observation function effectively. This need is reinforced by the emergence of new forms of threats such as hypersonic, swarming, miniaturised or stealth weapons, which require increased speed, sensitivity or accuracy of the recognition systems. This need applies to manned and unmanned platforms as well as to wide-area or long-lasting surveillance.

Besides, databases are essential for training, testing and certifying artificial intelligence (AI) systems such as image recognition systems. However, collecting data that is both representative of military operational scenarios and sharable for AI system development is a complex task. Furthermore, data annotation (e.g., definition of regions in images, labelling...) and curation need significant efforts that are often underestimated. The lack of specialised entities missioned to serve the community by actively creating representative and sharable databases further hinders the creation of such databases. These issues are often a bottleneck in system development. Frameworks should be developed that enable or facilitate cooperation and sharing of image databases for defence.

In addition, new high-resolution sensor technologies provide larger amounts of information that are difficult to transmit in their entirety in real time. Automatic processing located near the sensor is needed to reduce the information flow. This requires joint optimisation of software and hardware and can involve trade-offs between recognition performances and integration constraints.

Scope and types of activities

Scope

Proposals should address the development and objective testing of image recognition systems for defence, the creation of the needed new databases, and the integration of the developed image recognition technologies near the sensors and objective testing of these integrated systems. Any relevant types of images and sensors (visible, infrared, multiband, hyperspectral...) and any well-defined types of recognition tasks (detection and classification for well-defined classes of objects, detection and identification of known objects, tracking...) can be considered.

Types of activities

The following types of activities are eligible for this topic:

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)	Yes (mandatory)
(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 (mandatory)
(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 design has been developed, including partial tests for risk reduction in an industrial or representative environment	Yes (optional)

(e)	System prototyping of a defence product, tangible or intangible component or technology	No
(f)	Testing of a defence product, tangible or intangible component or technology	No
(g)	Qualification of a defence product, tangible or intangible component or technology	No
(h)	Certification of a defence product, tangible or intangible component or technology	No
(i)	Development of technologies or assets increasing efficiency across the life cycle of defence products and technologies	No

The proposals must address in particular the following:

- Creation and sharing of annotated image databases, and development of appropriate frameworks for that purpose
- Development of software image recognition systems
- Integration of such software systems on customised hardware near sensors (integrated technology demonstrators)
- Objective evaluation of the performances of the software and integrated systems

Functional requirements

The proposed solutions should fulfil the following requirements.

- A limited number of well-defined use cases should be addressed (possibly one).
- For each use case addressed:
 - o The use case should address well-identified military operational needs and scenarios.
 - o The use case should be defined by clear evaluation data, metrics and protocols described in the proposal. Evaluation raw data should be real images directly acquired through sensors. However, if real images do not yet exist (for instance for future threats) but hybrid or synthetic images can be expected to be representative of the anticipated threats, such images may be used.
 - o Several approaches should be explored by different research teams (while being evaluated in a comparable way using the above-mentioned data, metrics and protocols). The proposed techniques should be presented in the proposal.
 - o The state-of-the-art should be described in the proposal, relying as much as possible on past objective and quantitative evaluation results. The expected progress beyond the state-of-the-art should also be described, taking into account the foreseen amount of new training data and/or the ability to make a better use of existing data through innovative learning techniques, and a

possible roadmap toward technological maturity beyond the project should be provided.

- The needed image data should be collected, relying on dedicated trials and measurement campaigns as needed. Images should be annotated using documented annotation guidelines. The resulting databases should be shared at least with the project partners who need them in the framework of the project.
- The possibility to share and reuse these databases beyond the project should be anticipated, including where they would be classified. The organisational and technical framework for data production and sharing should be described in the proposal. In particular, the entity in charge of curating and distributing the databases should be clearly identified and the conditions for sharing should be described. If hybrid or synthetic images are needed for system evaluation, the possibility to share the tools used to generate these images should be anticipated in the same conditions.
- Setting up a framework for data production and sharing that can be reused beyond the project is encouraged. Synergies with similar efforts at the European level should be sought.
- Training and evaluation data should be representative of the use case and cover the various conditions encountered in real-life scenarios (e.g., various climate, weather or lighting conditions, various types of background landscapes...).
- If representative data that can be collected by users during operations is deemed needed to reach the expected system performance, machine-learning techniques to learn continuously from user supervision (user-driven adaptation) should be considered.
- Software recognition systems should be optimised to offer the best possible recognition performance (e.g., high probability of correct detection and low false alarm rates, high area under the ROC⁹ curve...).
- Integrated recognition systems should maintain the recognition performance of software systems as much as possible while taking into account size, weight, power and cost constraints.
- Both software and integrated systems should be benchmarked using the agreed-upon evaluation data, metrics and protocols.

Expected impact

The expected impacts are

- Shareable databases for image recognition
- Established frameworks easing the production and sharing of databases, creation or reinforcement of entities producing sharable databases
- Availability of new integrated image processing products

⁹ Receiver Operating Characteristic

- Enhanced decision-making and responsiveness, reduction of cognitive load of soldiers during operations
- Enhanced situational awareness
- Enhanced safety, resilience and survivability
- Reduction of fratricides and collateral damages
- Enhanced unmanned system autonomy

2.1.8. EDF-2022-RA-ENERENV-CUW: Sustainable components for underwater applications

- **Indicative budget:**

The Union is considering a contribution of up to EUR 20 000 000 for this topic under the call EDF-2022-RA

- **Number of actions to be funded:** Up to one action may be funded for this topic

Objectives

Piezoelectric materials used for military applications, especially in underwater acoustics, are to a very large extent based on ceramics, more specifically, on lead titano-zirconate $Pb_{1-x}Zr_xTiO_3$ (PZT). Civilian and military users now face challenges with European regulations regarding lead and its derivatives identified in the Candidate List of the Registration, Evaluation, Authorisation and Restriction of Chemicals (REACH) regulation from 2012, with the risk of its inclusion in the Annex XIV (substances under authorization) in the coming years. This is a concern for sonar systems used in underwater applications utilising piezoelectric ceramics. In addition to the REACH regulations, other global regulations, such as the Restriction of Hazardous Substances (RoHS) or Waste Electrical and Electronic Equipment (WEEE), require the elimination of lead and its salts from consumer goods and industrial devices. These constraints and regulations stimulate the need for an increased technological and industrial maturity of piezoelectric material alternatives to PZT. As an example, the recent update of the European RoHS directive has precluded the use of PZT ceramics from July 2021 for civil applications.

General objective

The general objective is to replace existing PZT based ceramics with alternative technologies, such as lead-free piezoelectric materials (aspiring to have no reduction in performance levels with even the potential for a gain), which will be suitable for military underwater applications, including the most demanding, which is a passive hydrophone and active transducer for sonar and underwater communications. The overarching goal is to have the emergence of at least one European lead-free piezoceramic supply chain, which will soon be mandatory with regarding the European REACH regulations. The patenting of new formulations and processes would be of use for sonar applications.

PZT ceramics are used in most acoustic sensors for underwater military applications: hydrophones, sonobuoys, dipping sonars, variable depth and hull mounted sonars, torpedoes, towed arrays. With the launch of major fleet renewal programs, which are currently entering

the implementation phase, the R&D of the naval sector has the challenge to control the environmental impact and the safety of ships, while preserving acoustic performance.

Since the renewal of scientific work on the replacement of PZT, started around 2000, considerable research has been conducted in studying substitution ceramics, with promising results. Research on demonstrators integrating lead-free piezoelectric ceramics and crystals based on BT¹⁰, KNN¹¹, KN¹², BCTZ¹³ has been published in scientific literature. However, gathering all the properties of PZT materials to alternative lead-free piezo-electric materials has never been done, and this is the reason academic research is still extremely active in this sector. In addition, reproducibility and process up-scale raise numerous issues.

Apart from military sectors, civilian markets are very broad and extend to several domains (non-destructive control sensors, medical echography apparatus, automotive, printing, energy harvesting). Even if civilian markets are very broad and potentially less demanding in terms of physical and piezoelectric properties than military domains, very few lead-free piezoelectric materials are proposed at industrial level and their physical and piezoelectric properties are very far from PZT. This means that mastering the production of advanced and high performance lead-free piezoelectric materials at an industrial level remains challenging. For the time being, no lead-free solutions exist that facilitate the high level of performance required by military underwater applications.

Specific objective

The specific challenge is thus to advance the state-of-the-art in the research of, and innovation in, new high performance lead-free piezoelectric materials for military underwater sensors applications to replace PZT, with a view to future phases of development and industrialization, leading to the prospective establishment of at least one European supply chain in this domain.

New materials can also provide the opportunity to generate additional benefits, for example, enlarging the operational frequency bandwidth of sensors or source generators, improving duty cycle limitations or reducing the sensor size. These opportunities can upgrade the performance of the sensors and should hence be considered in the evaluation of materials and processes to be studied.

Scope and types of activities

Scope

The proposals should carry out research actions for the development of advanced lead-free piezoelectric materials with physical and piezoelectric properties, enabling the substitution of PZT in military underwater applications. These research actions may be extended to disruptive ceramic technology processes, such as 3D printing, and material engineering to enhance current piezoelectric properties. Moreover, increasing the technological maturity of lead-free piezoelectric materials for PZT substitutions in military underwater applications, and assessing these new materials for military underwater applications on representative test transducers could also be considered. Furthermore, increasing the manufacturing readiness level of promising lead-free piezoelectric materials and enabling one or more European

¹⁰ Barium Titanate
¹¹ Potassium Sodium Niobate
¹² Potassium Niobate
¹³ Ba_{0.85}Ca_{0.15}Ti_{0.9}Zr_{0.1}O₃

industrial suppliers of lead-free piezoelectric materials for sonar transducers is a benefit of research activities in this area. In addition, the proposal must pay particular attention to potential synergies and complementarity to other ongoing R&D projects at national, multinational and on-going dual-use initiatives at European Union level, to avoid unnecessary duplication.

Types of activities

The following types of activities are eligible for this topic:

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)	Yes (mandatory)
(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 (mandatory)
(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 design has been developed, including partial tests for risk reduction in an industrial or representative environment	Yes (optional)
(e)	System prototyping of a defence product, tangible or intangible component or technology (prototype)	No
(f)	Testing of a defence product, tangible or intangible component or technology	No
(g)	Qualification of a defence product, tangible or intangible component or technology	No
(h)	Certification of a defence product, tangible or intangible component or technology	No
(i)	Development of technologies or assets increasing efficiency across the life cycle of defence products and technologies	No

The proposals must cover the following activities:

- Generating knowledge, with in particular:
 - o The review of the scientific and industrial state-of-the-art lead-free piezoelectric materials and innovative synthesis processes

- The identification of the relevant materials and processes
- The identification of manufacturing technologies for lead-free piezoelectric materials
- The review of the available operational specifications
- The definition of a roadmap for materials and processes development
- Integrating knowledge, with in particular:
 - The identification and assessment of EU industrial suppliers for the production of lead-free piezoelectric materials, including technology transfer.

In addition, proposals may address:

- Studies, with in particular:
 - The formulation, synthesis, physical and structural characterization, piezoelectric characterization of new composition of lead-free piezoelectric material.
 - The study of innovative process alternatives to current ceramic machining and advanced sintering processes.
- Design, with in particular:
 - The material specifications and advanced material characterization (piezoelectric tensor measurement) at sample and transducer levels.
 - The integration of parameters in transducer modelling, fabrication of representative transducer, which should be partially tested in real environmental conditions (e.g., assessment of linearity response with respect to stress and temperature, pressure and temperature cycling, endurance tests).

Functional requirements

The research to be conducted should meet the following functional requirements:

- Replace PZT by lead-free suitable piezoelectric materials and assess their performance level, aspiring to have no loss in performance or even a potential gain, against the following (not exhaustive):
 - For Active transducers: maximal Source Level, matched electrical bandwidth, power density, efficiency, and more generally for high drive, temperature, stress and electric field handling, duty cycle, power linearity
 - For Passive transducers: signal to noise ratio, stress handling (depth rating/for deep-sea applications), frequency bandwidth, and sensitivity.
- The choice of lead-free piezoelectric materials may differ depending on military underwater applications (passive or active transducers), and different use cases should

be addressed. For both use cases (active, passive), the loss, or gain, versus actual PZT transducers will be addressed through a redesign phase of equivalent lead-free transducers. These lead-free transducers shall undergo a series of pre-qualification tests (not exhaustive):

- Functional evaluation: source level, signal to noise ratio, sensitivity, frequency bandwidth, directivity, efficiency, linearity with power, endurance test
- Environmental evaluation: pressure and temperature cycling, vibrations, shocks.

Expected impact

The research should contribute to:

- reduction in pollution, which is a part of the European Green Deal,
- Strong technological differentiators compared to non-European sonar suppliers,
- Emergence of one or more European supply chains,
- Patenting of new formulations and processes,
- Compliance with REACH regulations on hazardous substances and obsolescence anticipation,
- Sustainability components for underwater applications

2.1.9. EDF-2022-RA-MATCOMP-PACOMP: Packaging technologies for critical defence components

- **Indicative budget:**
The Union is considering a contribution of up to EUR 20 000 000 for this topic under the call EDF-2022-DA
- **Number of actions to be funded:** Several actions, addressing different solutions, may be funded for this topic

Objectives

General objective

Future defence systems that target information superiority, new communication capabilities, new battlefield operations, combat capabilities and inter-theatre air operations require electronic components with high performance and multiple functionalities. Systems such as radiofrequency (RF) sensors for radars or electronic warfare systems, intelligent processing platforms or hardware-secured/cyber-secured modules need to be highly integrated and to fulfil specific military requirements. A particular challenge for defence forces is the digital control of the RF spectrum. For example, digital radar equipment will be driven mainly by components like analog-to-digital converters (ADC), digital-to-analog converters (DAC), the RF frontend, which will be mainly characterised by a transmit (high power amplifier - HPA) signal chain and a receiver (low noise amplifier - LNA) signal chain, and a robust switch, setting the mode of operation.

Specific objective

The performance of such a system will not only depend on the performance of the single chips used for each component but also on the quality and efficiency of their integration into packages and the optimization of their interplay with respect to the targeted application. Advanced packaging technologies are key to obtain compact, robust and reliable electronic components by integrating and encapsulating multiple electronic chips. The resulting Multi-Chip Modules and/or System in Packages (SiP) can provide high performance and multiple functions. Packaging with short interconnections between components minimizes parasitic elements that degrade signal integrity. This is particularly relevant for next generation radio-frequency application (e.g., radars or electronic warfare systems). Furthermore, an advanced density of integration allows hiding sensitive signals and integrating protection features, which is relevant for anti-tamper and secure module solutions.

Packaging technologies can also increase the resilience of supply in key technology areas, reducing dependence and improve security of information by allowing the use of components of different technologies and from different sources within a quality and security assured process. This is particularly relevant for defence applications for which securing the EU supply chains of critical electronic components is challenging due to small manufacturing volumes and potential constraints such as export restrictions.

Scope and types of activities

Scope

The topic addresses advanced System-in-Package technologies and architectures that take into account needs of defence systems with a particular focus on radio-frequency applications. It addresses improvement of packaging technologies, the preparation of design tools and the preparation of pilot lines.

The System-in-package should contain various types of elements (e.g., passives, high-speed digital components, ADC, DAC, memory components, microelectromechanical systems (MEMS), optical component) made of different materials (e.g., Si, SiGe, III/V semiconductors such as GaN and GaAs, RF complementary metal-oxide-semiconductor (CMOS)) and produced by different processes (semiconductors technology nodes both manufactured in the EU or Norway and outside.). A package should combine digital and analogue functions and integrate, if adapted to the considered application, further security functions and thermal management functionalities.

Proposals should strive to identify a supply chain from actors from the EU and Norway offering independent OSAT (Outsourced Semiconductor Assembly and Test) services, in order to reinforce an EU and Norway industrial sovereignty independent from any usage constraints. As appropriate, proposals should take into account different technologies (such as Fan-Out Wafer Level-Packaging – FOWLP etc.) for creating the System-in-Package.

Relevant use cases for defence applications include RF sensors (Radar, electronic warfare including high power source for jamming, millimetre wave communications), data security and smart sensors for ammunitions.

Size, weight and power dissipation are of high concern for embedded applications. Moreover, the use in harsh environment should be taken into account. This can include aspects of G-

hardening, shocks and thermal conditions, e.g., necessary for gun-launched applications or brutal landing on aircraft carriers.

This topic is linked to the sectoral analysis performed by DG DEFIS and studies performed by EDA in the framework of the CapTech TCM. Synergies between defence, space and civil technologies have to be taken account in order to avoid duplication costs.

Where applicable, proposals should build on skills, technologies and associated industrial capacities that are partially available in EU and Norway for defence or for civil applications. The proposals must substantiate synergies and complementarity with civil initiatives, notably supported by EU programmes in the space sector. It must avoid unnecessary duplications with other EU, intergovernmental or NATO initiatives.

Types of activities

The following types of activities are eligible for this topic:

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)	Yes (optional)
(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 (mandatory)
(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 design has been developed, including partial tests for risk reduction in an industrial or representative environment	Yes (mandatory)
(e)	System prototyping of a defence product, tangible or intangible component or technology (prototype)	No
(f)	Testing of a defence product, tangible or intangible component or technology	No
(g)	Qualification of a defence product, tangible or intangible component or technology	No
(h)	Certification of a defence product, tangible or intangible component or technology	No
(i)	Development of technologies or assets increasing efficiency across the life cycle of defence products and technologies	No

Among other tasks that the applicants deem necessary, the following tasks must be performed as part of the mandatory activities of the project:

- Integrating knowledge:
 - o Research activities on materials (e.g., innovative substrate), interconnect technologies and components for high-performance packaging, including tests of candidate technologies
 - o Research activities on the integration of heterogeneous components and necessary interfaces, including experimental testing.
- Studies
 - o Evaluation of different modular architectures and targeted platform technologies (such as FOWLP)
 - o Identification of chiplets categories needed for relevant defence applications such as RF sensors, digital security, IMU (Inertial Measurement Units), etc.,
 - o Definition of relevant chiplet interfaces that enable integration of the chiplets in advanced packaging, taking into account open initiatives focussing on civil applications for standard functionalities.
 - o Assessment of requirements and common candidate technologies for a wide range of different defence applications, and specifically the interface between die and package to ease integration of chiplets
 - o Definition of a test strategy to ensure safety and security standards for low-volume heterogeneous integration
 - o Taking into account the outcome of the design activities, identification of the best supply chain per technology and use case application (sensitive or not) compatible with real production (Manufacturing Readiness Level aspect)

Proposals may additionally include the following tasks under this activity:

- o Study on the set-up and management of a shared library for chiplets
- Design
 - o Definition of System-in-Package modular architectures, including those based on chiplets, supporting RF sensors, digital security, inertial measurement units (IMU), etc., and technologies for functions with military specificities
 - o Define design methodologies and set up physical design kits (toolbox, modular physical design kits, multi-physics design) for the targeted technology platforms, taking into account the specificities of military systems.
 - o Design of physical interfaces for components (or chiplets) that optimize integration in the package.
 - o Design of selected common interface protocols for components (or chiplets) that enable reuse and optimize integration in next generation SiP platforms

- Develop demonstrators of common interface test chips (such integrated passives including switches, protocol bridges and links, test structures...), integrate and test them on a SiP technology demonstrator platform
- Design of test structures that can ensure safety and security standards for low-volume heterogeneous integration
- Design of technological demonstrators taking into account the defined use cases
- Testing in at least two iterations of the technological demonstrators, including reliability tests, for the evaluation on relevant platforms and including a failure analysis, if applicable.
- Design of a pilot line, including the strategy of test and feasibility tests.

Functional requirements

Proposals should address technologies and solutions that fulfil the following requirements:

- Compatibility with several defence applications, including active electronically scanned array (AESA) radar preferably targeting X-Band and above, electronic warfare including high power source for jamming, millimetre wave communications, data security and smart sensors for ammunitions
- Optimization for radio-frequency applications with high-power, low signal
- Modularity and configurability to meet various requirements of different military applications.
- Optimization of size, weight, cost and power dissipation capability
- Integration of solutions against reverse engineering and enemy observation (like anti tampering and tempest)
- Compliance with the Registration, Evaluation, Authorisation and Restriction of Chemicals (REACH) and Restriction of Hazardous Substances (ROHS) regulations
- Compliance with the military standards (e.g., MIL-STD 810...) for the target applications (e.g., taking into account requirements for aviation certification), in particular with respect to harsh environments, G-hardening, shocks and extreme thermal conditions

Expected impact

- Increase level of skill and knowledge in the European Defence Technological and Industrial Base concerning advanced packaging
- Create System-in-Package reference architectures and technological solutions for next generation military systems
- Strengthen the independence and competitiveness of the European supply chain for low-volume technologies and solutions that fulfil military requirements by enabling a heterogeneous integration approach (combining European based semiconductor components and non-European advanced nodes components)
- Enhance security of information by defining adapted test strategies and methods for risk mitigation

- Guarantee the access to packaging services to the EU Member States and Norway
- Promote a collaboration network between EU Member States and Norway including academy, research centres and industry looking for synergies with civil initiatives.

2.1.10. EDF-2022-RA-PROTMOB-FMTC: Future mid-size tactical cargo aircraft

- **Indicative budget:**

The Union is considering a contribution of up to EUR 30 000 000 for this topic under the call EDF-2022-RA

- **Number of actions to be funded:** Several actions, addressing different solutions, may be funded for this topic

Objectives

Tactical transport aircrafts are the workhorses of battlefields, fulfilling missions like airdrop delivery, parachutist drop, logistics, medical evacuation (MEDEVAC), air to air refuelling, special missions under harsh and adverse conditions, which are critical for the success of military operations. Operations in hostile environments demand e.g., built in electronic warfare self-protection systems and set requirements on the platform performance/build up in order to be suitable for the task, and furthermore to operate with limited ground infrastructure (e.g., unprepared runways).

Beyond their pure military role, tactical transport aircrafts are also key assets for a better civil defence/protection and EU-internal needs, with critical contribution to disaster relief, search-and-rescue and sanitary crises response.

Beside the A400M, which is on the high-performance side of the capacity, the initial conception of the majority of currently operating tactical aircraft (C130, C-295, C-27J ...) is now 40 years old, and there is a need for a new medium tactical European aircraft, lighter than the A400M that could provide a complementary capacity for tactical transport.

Currently, some EU Member States are operating medium payload tactical military transport aircrafts within their fleet, which can be replaced with growing capabilities, able to cope with the envisaged operational challenges.

The Future Mid-size Tactical Cargo aircraft (FMTC) feasibility study proposal for EDF 2022 addresses this coming strategic gap within the European transport portfolio. FMTC proposes a cooperative analysis of the transport aircraft replacement needs on the 2030-2050 horizon and the identification of European development opportunities, among the EDF participating Member States and associated countries.

This topic is an opportunity for Europe to federate efforts by providing the EU defence community (nations and industry) with robust elements to decide what the 2035+ future of EU military tactical transport could be.

Scope and types of activities

Scope

The scope must cover the feasibility study phase of the possible development of a future tactical transport aircraft.

Proposals must include at least the following activities:

- Feasibility Study for one or two aircraft, depending on the convergence on the requirements by the participating Member States and associated countries;
- Preliminary requirements review (PRR) accepted by the cooperating Member States and associated countries, which will confirm the technical, programmatic, industrial and market feasibility of the analysed solutions, giving participating States all necessary elements to select the aircraft configuration that could be carried forward through a development and industrialization phase.

Types of activities

The following types of activities are eligible for this topic:

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)	Yes (optional)
(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 design has been developed, including partial tests for risk reduction in an industrial or representative environment	Yes (optional)
(e)	System prototyping of a defence product, tangible or intangible component or technology	No
(f)	Testing of a defence product, tangible or intangible component or technology	No
(g)	Qualification of a defence product, tangible or intangible component or technology	No
(h)	Certification of a defence product, tangible or intangible component or technology	No
(i)	Development of technologies or assets increasing efficiency across the life cycle of defence products and technologies	No

In particular, proposals must address:

a- Technical activities:

- Definition and assessment of the candidate aircraft solutions (one or two aircraft alternatives);
- Assessment of the preliminary technical specifications, concept studies and sizing for major sub-systems (propulsion, avionics and general systems);
- Identification of critical technologies for technical and economic feasibility, and proposal of pre-development plans. Specific areas of interest are:
 - o design and manufacturing technologies to reduce acquisition and maintenance costs;
 - o technologies towards lower or zero emission production and operation;
 - o technologies to improve operational availability.
- Identification of critical technologies to improve the operational capability in the domain of:
 - o take-off and landing in challenged environment;
 - o wide range and low consumption;
 - o self-protection capabilities;
 - o more autonomy;
 - o improved connectivity in the operational theatre.

b- Programme activities:

- Establish the preliminary programme management and the system engineering plans;
- Establish the overall programme schedule / roadmap;
- Perform a costing evaluation exercise;
- Perform a market assessment review;
- Identify risks and constraints related to implementation, costs, schedule, organisation, operations, maintenance, production and disposal;
- Identify key technological aspects and plan for their maturation within the programme plan.

c- Operations activities:

- Define the concept of operation;
- Define the sustainment model (i.e., number of planned flight hours, layout of bases, deployments);
- Define a baseline for aircraft logistic support.

d- Iterative definition of aircraft detailed requirements:

- Perform a mission definition review (MDR) and Preliminary Requirements Review (PRR).

e- For a subsequent design phase:

- Provide a proposal for a best candidate solution based on a complete value analysis covering performances, costs, risks, modularity, manufacturability, safety, consistency with Member States and Norway' operational needs, with jointly defined detailed criteria and hypothesis.

Functional requirements

The proposition of a new aircraft development would be based on:

(1) Intangible:

- European Geo return: Development and involvement of European industries, acting as tractor for many European aerospace companies and small and medium-sized enterprises (SMEs);
- Export opportunities: Custom made to fit EU partner's requirements, with open architecture to address worldwide opportunities;
- Based on operational scenarios & threat environment 2030+ (i.e., Multi Domain connectivity).

(2) Tangible:

- Affordability, in terms of acquisition and lifecycle costs. Operating costs below similar available solutions in the market;
- Operations in demanding unprepared runways, hostile environments and tactical intra theatre operations;
- Flexibility for operating different kind of military missions and possibly reconfigurable for supporting civilian needs;
- Logistics capability: ability to carry tactical vehicles that do not fit in existing solutions;
- Multi-mission capability: ability to act as a multi-mission transport platform and be customized for specific roles;
- State of the art development, ensuring availability and reliability of the platform and avoiding obsolescence concerns;
- Sustainability along the entire product lifecycle: from the conception / production by means of digitalisation up to the product use with reduced environmental footprint due to e.g., advanced propulsion system, low weight and more efficient flight capabilities.

Expected impact

- Reinforce the European strategic autonomy in the military transport segment;

- Develop vital military capabilities in highly contested environments (e.g., tactical transport, airdrop, air assault) against technologically advanced adversaries;
- Develop EU MEDEVAC capabilities and EU disaster relief, and sanitary crisis response capabilities;
- Promote and protect the European technological and industrial ecosystem, based on a potential new aircraft development;
- Enhance cross-border collaboration (from large industrial groups to SMEs) through the opportunities offered by the several elements of the platform and its architecture.

2.1.11. EDF-2022-RA-UWW-UTS: Underwater manned-unmanned teaming and swarms

- **Indicative budget:**

The Union is considering a contribution of up to EUR 25 000 000 for this topic under the call EDF-2022-RA

- **Number of actions to be funded:** Several actions, addressing different solutions, may be funded for this topic

Objectives

General objective

This topic addresses research for future capabilities addressing moving subsurface threats using manned-unmanned teaming and swarm technologies, possibly including surface and air platforms and components, particularly in confined and shallow waters (CSW). This System-of-Systems (SoS) should enable enhanced operational efficiency and performance. The actions in this topic should address state-of-the-art, and beyond, swarm control solutions. This includes analysis of centralised, distributed, and hybrid control models. Swarm control may employ control scheme with a global or local approach and their optimised combination. The control-scheme should adopt to mission type changes as the operation evolves from one phase to another. Guidance and control strategies for the swarm are also to be considered, where inductive and swarm internal cognitive-like self-control needs to be analysed.

Specific objective

The aim is to develop swarming technologies up to at least TRL 4 and validated in seawater. The expected result of the research activities performed with the support of this call is a better mission performance result than the one obtained by an individual UxV or platform alone. This should take into account data sources of opportunity. The main challenges or factors to be solved to enable this are the following:

- The SoS shares a common objective for all the individual components
- The SoS can be composed of systems, vehicles, and platforms of different nature and capacities
- The architecture and functions need to be derived and controlled by the task or mission aim that has been defined.

- The SoS architecture and protocols enables it to utilise resources outside the cooperative system.

Scope and types of activities

Scope

The proposal for research on swarm aspects of unmanned systems and the collaboration policies that govern it, performing underwater missions, in CSW, shall address, among others, the following aspects:

(1) Mission or task-based performance by the swarm and all its components. The definition, and management of the collaborative system, dependent on the architecture defined, will aim to optimize the use of every individual to better obtain the common objective. This will require planning and control with a focus on at least the following:

- a. Coordination and cooperation inside the system to share a defined space/environment and also the information obtained. Interoperability of the system within a defined architecture (centralized/decentralized).
- b. Adjust to changes in the environment and optimise accordingly, while maintaining mission objective.
- c. The cooperation of heterogeneous vehicles will involve the integration of a large amount information provided by different sensors.
- d. The information obtained about the environment or operation must be combined, analysed and disseminated in real time in order to provide feedback to the system through interoperability standards, which should be consistent with relevant NATO standards.
- e. Communication: A Shared link between vehicle and control station must be robust and reliable. Relevant protocols, such as JANUS underwater communications protocol must be taken into consideration.
- f. Providing the HMI-infrastructure to control the system, taking into account different levels of autonomy.
- g. The definition of the behaviour model of every individual inside the system and of different swarm collaborative models, e.g.: One mission shared by the platforms of the swarm; or swarm split in two or more squads with their own missions

(2) Participation of vehicles with different characteristics: The use of different platforms will allow the use of different capacities taking into account several aspects such as:

- a. Level of autonomy and combinations of different levels
- b. Movement (kinetic) characteristics
- d. Types of platforms (UUV, USV, sonobuoys, gliders etc.)
- e. Enabling systems installed such as detect and avoid (DAA) systems (below and on the surface)
- f. Command, Control, and Communication Systems

g. In-swarm localisation, communication and coordination

h. Payloads, such as sensors and effectors

The proposed solution must give due consideration to the need to cooperate with other platforms to achieve a common goal (interoperability, information processing, security in operation, communication, detect and avoid, etc.). The resulting cooperation policies need to integrate all the existing with the new challenges arising from this kind of operation.

The proposal must give due consideration to techniques of cooperation between unmanned autonomous systems when acting as a swarm, namely task allocation/mission/route optimisation algorithms. Other, novel methods are also encouraged and invited to this topic.

Proposals that envisage unmanned and autonomous systems to work together as a squad - rather than as a swarm- (i. e each system/platform is performing a different task) are also welcome. Then the task allocation problem must be solved as well as the automatic re-tasking of the whole squad or group and each single unmanned asset. It should then also propose a solution for the automatic reconfiguration of the squad. The method of hierarchical task networks, or the method of intelligent software agents for implementing cooperation between systems/platforms can be used, but any other, alternative method can also be proposed.

An analysis and the elaboration of policies of cooperation between unmanned systems (swarming) should be described in detail in the proposal.

Appropriate level of human control must be respected also in proposals containing solutions with autonomous features.

The proposal should address SoS architecture, control, and guidance solutions of unmanned systems (swarming) and/or unmanned and manned systems in the underwater domain. This includes:

- Combinations of autonomous sub-swarms or squads of heterogeneous unmanned vehicles that cooperate and collaborate to complete different types of missions (for example anti-surface warfare ASuW, anti-submarine warfare ASW, intelligence surveillance and reconnaissance ISR, MCM, Mine-laying and transport).
- An analysis of the general aspects of the operation of a cooperative system of unmanned vehicles and platforms, where the SoS may draw upon resources available to it from systems outside the cooperative system.

Types of activities

The following types of activities are eligible for this topic:

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)	Yes (mandatory)

Types of activities (art 10(3) EDF Regulation)		Eligible?
(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 (mandatory)
(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 design has been developed, including partial tests for risk reduction in an industrial or representative environment	Yes (optional)
(e)	System prototyping of a defence product, tangible or intangible component or technology (prototype)	No
(f)	Testing of a defence product, tangible or intangible component or technology	No
(g)	Qualification of a defence product, tangible or intangible component or technology	No
(h)	Certification of a defence product, tangible or intangible component or technology	No
(i)	Development of technologies or assets increasing efficiency across the life cycle of defence products and technologies	No

The proposals must include generating knowledge, integrating knowledge, and studies activities. The proposal may include design activities.

The proposals must substantiate synergies and complementarity, while avoiding duplication, with concepts and architectures developed in complementary ongoing European work streams and projects where relevant.

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

- Articulation, and if necessary, development, of relevant military scenarios, that will form the basis for development of solutions.
- Improvement and creation of knowledge by in-depth research in the form of studies that address the most critical technology gaps to enable capabilities for swarms to function in dynamic underwater environments while performing military tasks. Also research topics that address other specific shortfalls of manned-unmanned teaming in the context of swarms with autonomous features must be addressed.
- The feasibility of developed solutions based on the in-depth research must be explored through technological demonstrations, trials and/or simulations in relevant military scenarios. The demonstration must include seawater (underwater) tasks for relevant

parts. A final demonstration will serve as an instrument to show the industrial state-of-art performance to the military community, visualize the results of the targeted research activities, present potential military value and identify technology shortfalls that need to be addressed in subsequent activities in nations and EU

Functional requirements

The solution should enable swarm configuration optimisation taking into account mission and task, resources, environment, military scenario and threat.

The swarm, sub-swarm, individual and node control solutions should enable obstacle detection and avoidance, reconfiguration in case of failure of individuals or nodes, behaviour in case of loss of communication.

The solution should facilitate swarm control and guidance for swarm sizes up to several hundreds of individuals in multiple sub-swarm configurations.

The solutions should enable mission performance with loss of individuals, communication and control.

The solution should enable functionality in GNSS degraded and cyber contested environment.

The solution should enable in-swarm localisation and coordination. The solution should be interoperable with existing standards when relevant, including NATO standards.

Collaborative systems composed by multi domain platforms (UUV, USV, sonobuoys, gliders, etc.) operating together may face several challenges. The solution should enable:

- Ensuring bidirectional communications link between the subsea units and the mother ship or ground control station.
- Ability to use own sensors (such as towed SSS/deployable sonars, etc.) to carry out the mission of subsea monitoring, while being able to cooperate with other platforms and systems
- Ability for USV to carry on board a set of UUVs to be rapidly deployed in a certain surveillance area at relevant distance from the ship.

Expected impact

It is expected that the outcome should:

- Strengthen the European defence technological and industrial base (EDTIB) on technologies related to unmanned and autonomous swarming technologies that operate both above and below the water.
- Generate knowledge to fill capability gaps in use of underwater manned –unmanned teaming and swarms in support of naval operations
- Contribute to the interoperability and future capabilities of European forces in the area of swarm solutions for mission execution in the naval domain, including in particular the underwater domain.

2.1.12. EDF-2022-RA-UWW-ODAC: Underwater observation, detection, acquisition and communications

- **Indicative budget:**

The Union is considering a contribution of up to EUR 30 000 000 for this topic under the call EDF-2022-RA

- **Number of actions to be funded:** Up to one action may be funded for this topic

Objectives

General objective

Timely and robust detection and monitoring of moving underwater threats (such as submarines, swimmer delivery vehicles (SDV), combat divers, underwater unmanned vehicles (UUV)) in open sea and coastal waters is critical for maintaining sea control, for ensuring freedom to operate own forces, for A2AD operations, for harbour protection, for force protection, and for protection of critical national infrastructure.

Future capabilities need to be effective, mobile, adaptive, scalable, and flexible to counter threats from the underwater domain, leading to new technical and conceptual solutions to be developed. As traditional naval ships will become an increasingly scarce and expensive resource and will not be sufficient to provide the necessary geographical coverage and flexibility needed for the future, research is required on modular unmanned systems for underwater warfare with prerequisite principles of unmanned air, surface and underwater (UxV) standards.

Specific objective

Underwater communication, detection, and monitoring of moving targets are common denominators for traditional warfare areas such as Anti-Submarine Warfare (ASW), underwater surveillance, harbour protection, and seabed warfare. Mission specific sensor solutions and tactical approaches differ in these, despite having common denominators. Timely detection of moving underwater threats at sufficient range is identified as one of the biggest challenges. Providing technical solutions for underwater target detection, allowing to prepare appropriate reaction to a subsurface threat, will therefore impact the whole range of warfare areas mentioned above. The aim is to develop technological novelties at least up to TRL 5.

Scope and types of activities

Scope

The proposal for research on underwater observation, detection, acquisition and communications is expected to make an evaluation of critical technologies for detection of underwater threats for protection of maritime infrastructures and coastal strategic areas and assets, and identify novel technologies for improved situational awareness. This assessment of individual technologies will in a first stage be integrated to demonstrate an improved capability in underwater surveillance in littoral waters. This does not exclude open sea as an environment of operational use for the capability.

The proposal must cover at least the following parts:

- The first part is a scientifically focused part of research topics that today represent critical shortfalls in the process chain from sensor to underwater situational awareness and challenges in coordinated operation of unmanned system-of-systems. A strong emphasis is on the scientific quality and relevance of these identified research topics. Technology areas and solutions for specific underwater missions, excluding MCM, that must at least be considered are: sensor systems for the detection of underwater threats at long ranges; processing methods for noise attenuation and automated target detection; technologies for target classification, positioning, tracking, and target identification; autonomy and autonomous adaptive operation of UxV; System-of-system architecture and interoperability standards; Command, control, communication and information systems in support of operations
- The second part is a comprehensive demonstration of the project results in a realistic scenario at sea, adapting them to existing UxVs, sensor and communication systems, infrastructure components, and data management systems¹⁴.

An overall system-of-systems (SoS) approach must be used that puts together experimental configurations of unmanned mobile sensor platforms, rapidly deployed distributed autonomous nodes, ad-hoc underwater and radio communication networks together with an overall combat management system (CMS) for establishing situational awareness of the underwater threat.

Different components of the system of systems are expected to bring increased flexibility through a modular toolbox, comprising a range of systems focused to be deployed as autonomous sensors or to be adaptable to existing or newly developed maritime platforms.

Appropriate level of human control must be respected also in proposals containing solutions with autonomous features.

Types of activities

The following types of activities are eligible for this topic:

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)	Yes (optional)
(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)

¹⁴ The use and adaption of existing systems in creating new intellectual property must take into consideration provisions on 3rd party IP ownership (EDF regulation article 20).

Types of activities (art 10(3) EDF Regulation)		Eligible?
(d)	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, including partial tests for risk reduction in an industrial or representative environment	Yes (mandatory)
(e)	System prototyping of a defence product, tangible or intangible component or technology (prototype)	No
(f)	Testing of a defence product, tangible or intangible component or technology	No
(g)	Qualification of a defence product, tangible or intangible component or technology	No
(h)	Certification of a defence product, tangible or intangible component or technology	No
(i)	Development of technologies or assets increasing efficiency across the life cycle of defence products and technologies	No

The proposals must include study and design activities. The proposal may include generating knowledge and integrating knowledge activities.

The proposals must substantiate synergies and complementarity, while avoiding duplication, with concepts and architectures developed in complementary ongoing European work streams and projects where relevant.

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

- For studies, supported by experimentation: In-depth research that address the most critical technology gaps to enable capabilities for underwater detection, classification, tracking and surveillance of underwater moving targets, as well as to enable capable and reliable communication links within the SoS.
- For design, including demonstration: a final comprehensive SoS demonstration involving state-of-art unmanned and autonomous systems that may be configured to represent a complete process chain from detection-to-awareness, playing a realistic military scenario and using realistic moving targets in real environmental conditions. The demonstration must implement results from the scientific studies in such a way that the impact of each of the studies has a potential operational capability, will be clearly visible in the demonstration. In addition, sub-systems to the SoS should be demonstrated.

The tasks must address at least:

- Methods, technologies, systems and devices for the detection of underwater moving threats at long ranges, their classification, positioning and subsequent tracking. These have to consider covert detection solutions, such as multi-static and distributed systems. Also automated target detection has to be addressed. In addition, methods related to mitigation of environmental influence on detection have to be addressed.

Autonomy and autonomous adaptive solutions to ameliorate the probability of detection, classification, positioning and tracking of underwater moving targets have also to be addressed.

- Methods and technologies for robust and resilient communication for an underwater system of systems with the aim to establish situational awareness of the underwater threats

A final demonstration will serve as an instrument to show to the military community the results of the targeted research activities, present potential military value and identify technology shortfalls that need to be addressed in subsequent activities in nations and in EU.

The SoS design must respect an open architecture approach and interoperability standards.

Additional tasks may address other specific shortfalls in unmanned and autonomous technologies and coordinated operation of SoS may be addressed. The following tasks may be performed as part of the eligible activities:

- Research on novel technologies for accurate target positioning and tracking. These may include solutions for active and passive arrays and towed arrays mounted on unmanned vehicles (UxV).
- Research on Command, control, communication and information systems in support of operations. For underwater communication: signal processing using novel processing techniques for robust, long range and adaptive communication, including adaptive networks. These can include novel techniques and standards for the implementation of next-generation underwater communication networks.
- Research on enablers for autonomous operations of UxVs in order to develop a consistent preliminary operational system of systems - such as; robust precision navigation, adaptive behaviour, long endurance (high efficiency energy sources), launch & recovery (e.g., UxV deployment platforms - such as military vessel specially designed to launch and recover naval UxV), underwater infrastructure networks
- Research on Human machine interface (HMI).
- Research on Internet of Underwater Things (IoUT, or UIoT) applications including all characteristic layers of IoUT (perception, network and application) and approach to solve the challenge of detection of underwater threats at long distance.

Functional requirements

The proposal should meet requirements for demonstrating a military scenario where detection, acquisition, and timely communication of underwater threats represent the core innovation part of the project.

The proposed solution should:

- Improve and speed up detection, tracking and classification of underwater moving threats especially in most demanding conditions and complex environments (coastal areas, reverberations, maritime traffic, sea state, environmental noise)
- Involve improved or new generation of sensors (active / passive sonar, magnetic anomaly detectors (MAD), hydrophones, active and passive sonobuoys, etc.).

- Have improved capabilities for underwater data connectivity to other equipment (tactical systems, multiple sensor-data fusion configurations) including in cyber-contested environments.
- Be interoperable with existing standards, where relevant, including NATO standards.
- Offer a modular and flexible design to ease the integration of new sensors and effectors (to ensure high scalability in terms of integration with existing or new sensors, effectors and subsystems)

Expected impact

It is expected that the outcome should:

- Strengthen the European defence technological and industrial base (EDTIB) on technologies related to unmanned systems, autonomy and the system-of-systems infrastructure needed to demonstrate situational awareness related to moving underwater threats.
- Identify specific research topics and generate knowledge to fill capability gaps in underwater threat assessment.
- Contribute to the interoperability and future capabilities of European forces in the area of underwater communication, detection, and monitoring of moving targets.

2.2. Call EDF-2022-LS-RA-DIS

- **Targeted type of actions:** Research actions (dedicated to disruptive technologies for defence)
- **Form of funding:** Lump sum grants following the call for proposals
- **Targeted type of applicants:** Any consortium of eligible entities as defined in Article 9 of the EDF Regulation and involving at least two legal entities established in at least two different Member States or associated countries. At least two of the eligible legal entities established in at least two Member States or associated countries shall not, during the entire period in which the action is carried out, be controlled, directly or indirectly, by the same legal entity, and shall not control each other.
- **Indicative budget for the call:** The Union is considering a contribution of up to EUR 40 000 000 to support the following 3 call topics:

2.2.1. EDF-2022-LS-RA-DIS-AC: Innovative technologies for adaptive camouflage

- **Indicative budget:** the Union is considering a contribution of up to EUR 15 000 000 for this topic under the call EDF-2022-LS-RA-DIS.
- **Number of actions to be funded:** several actions, addressing different solutions, may be funded for this topic.

Objectives

Camouflage is an important measure to protect soldiers and military platforms. The adaptation of the camouflage characteristics to the conditions, such as encountered sensors, environment and threat level, could bring this protection to a new level. Both the performance of the adaptive camouflage and material characteristics, including its passive properties (e.g.,

fire/electric shock protection and camouflage), will influence the impact of this technology on military capabilities. This topic complements ongoing projects, in particular following the PADR call on research in technology and products in the context of Force Protection and Soldier Systems.

General objective

The threats' fast adaptation, hybridization, proliferation of innovative technologies, and increasing lethality of threats, highlight the importance of enhancing the Land Systems (both soldiers and platforms) protection. Lower mass better protected military platforms and soldiers are easier to operate at reduced risk for injuries.

An important measure to protect soldiers and military platforms is camouflage in a wider spectral range, also including radar frequency bands¹⁵.

Specific objective

A good camouflage coverage changes the appearance or signature respectively and prevents from being detected, recognized or identified, and furthermore from being, attacked, hurt, killed, damaged or destroyed. Various camouflage measures have been used in many conflicts and have led to partially astonishing and impressive results. Legacy camouflage techniques and means are normally passive materials with fixed technical properties and with no possibility to adapt or change them. Hence, the signature remains unchanged if the background changes due to movement for example. These conventional techniques are being used in nearly all military situations, missions, scenarios and environmental conditions.

At the same time, available military and commercial sensors, drones, detectors and cameras in combination with sophisticated signal or image processing and analysing software algorithms (such as artificial intelligence-based routines) increase the probability to detect, to recognize or to identify such conventionally camouflaged objects. An increasing threat consists of (more) affordable high-tech sensors, airborne (e.g., drones) and ground based, operating in the spectral bands mentioned in footnote 16, including emerging sensor technologies (such as lasers scanning and quantum) and multi and hyperspectral sensors.

Improved and new Camouflage, Concealment, Deception & Obscurant (CCD&O) solutions and operating procedures are required to prevent land systems (including their weapons) to be detected, identified or their intentions disclosed. Potential countermeasures include passive camouflage, mobile systems, weapons, active camouflage, including smart materials, deception methods, obscurants, and deceptive technologies.

A promising contribution to this challenge is adaptive camouflage techniques and devices that are able to adapt their signatures to the background, to the surveillance sensors (mainly when active), different weather and daytime conditions and threat level hence reducing the ranges of detection, tracking, recognition and identification increasing the survivability of soldiers and platforms. Military platforms or soldiers equipped with adaptive camouflage measures are able to change the signature and to adapt it to the actual background or to deceive sensors in different spectral bands. In order to provide protection against future sensor technologies, development of new materials and concepts have to be investigated. The current development

¹⁵ Spectra of interest for this topic include ultraviolet radiation (100-380 nm), visible radiation (380-780 nm), Near infrared (0.75–1.4 µm), Short-wavelength infrared (1.4–3 µm) Mid-wavelength infrared (3-8 µm) and Long-wavelength infrared (8-15 µm) along with radar bands X (8–12 GHz), Ka (27-40 GHz) and W (75-119 GHz).

of electromagnetic detection tools like Foliage Penetration Reconnaissance, Surveillance, Tracking and Engagement Radar pinpoints a need for wider spectral range protection, also including radar frequency bands, to protect moving soldiers or military platforms under trees. A combination of camouflage in the optical and radar spectral bands will ensure the highest level of protection, reducing the risk of being targeted.

In that sense and in line with both ‘Ground Combat Capabilities’ CDP¹⁶ priority and ‘Soldier Systems’ CARD Focus Area, this topic aims to push the undergoing technological effort addressing adaptive camouflage for protection of land systems.

In particular - and in compliance with European Defence Agency (EDA)’s Overarching Strategic Research Agenda (OSRA) results, including TBB3¹⁷ “Passive and active protection for Land Systems” and TBB87 “Camouflage and Signature Management Technologies” - this topic will contribute for closing the technical gaps directly related with the following capabilities:

- Upgrade, modernize and develop Land platforms to adapt to operational environment
 - upgrade of current and development of next generation’s armoured platforms.
- Enhance protection of forces.
- Improve individual soldier equipment.

Scope and types of activities

Scope

The main scope is to investigate suitable adaptive innovative camouflage techniques, taking also into account usability, and to demonstrate this with a technology demonstrator in real applications. Especially the problem of a good adaptation to the background and to the observing sensors in different spectral bands should be at the heart of the activities. Proposals should address the development of new concepts, technological blocks, sub-systems and/or systems. Technologies for commercial, civil applications and concepts of previous projects that have been publicly presented should be taken into account.

In order to understand the prioritisation of adaptive camouflage techniques, the activities should contain a threat analysis, which explores and ranks risk areas on military platforms or soldiers and ranks spectral range threats to be treated. These considerations should reflect night-time and daytime scenarios, situations of degraded visual environment given in woodland, arid and snow situation. The abovementioned threat analysis should also contain reference on the physics of camouflage for each spectral band.

The activities shall further focus mainly on research on state-of-the-art and innovative adaptive camouflage techniques and devices in the different optical and radar spectral bands, on arranging and combining them in a common structure (layers, mosaic), on realizing a demonstrator (rigid panel display, elastic shield or flexible textile) and on testing and assessing it. The aim is to have the ability to change the signature (intensities and patterns) in different spectral bands at the same time without deteriorating the signature in any other spectral band. A concept and proposal to develop a self-adapting closed loop with the help of

¹⁶ Capability Development Plan

¹⁷ Technological building block

sensors (either embedded or as part of the material) detecting the surrounding environment and its own signature should also be planned. Materials for signature management in spectral bands listed in footnote 16 not deemed as threats should be studied on a more basic research level (TRL 1-4). Moreover, a development of bi-recyclable textiles and flexible elements (e.g., smart glass, optical fibres, etc.) with widest possible anti-radar properties should be investigated.

The adaptive camouflage techniques considered should address the integration with the platform or soldier C4I technology and should consider power source appropriate for the platform or soldier energy budget.

Types of activities

The following types of activities are eligible for this topic:

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)	Yes (mandatory)
(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 (mandatory)
(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 design has been developed, including partial tests for risk reduction in an industrial or representative environment	Yes (mandatory)
(e)	System prototyping of a defence product, tangible or intangible component or technology (prototype)	No
(f)	Testing of a defence product, tangible or intangible component or technology	No
(g)	Qualification of a defence product, tangible or intangible component or technology	No
(h)	Certification of a defence product, tangible or intangible component or technology	No
(i)	Development of technologies or assets increasing efficiency across the life cycle of defence products and technologies	No

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

- Generating knowledge
 - (1) threat analyses to prioritise object areas for each spectral band
 - (2) selection of suitable and development of innovative camouflage techniques and principles in the different spectral bands
 - (3) design of the materials or components with the aim of reducing the target's signature in all the considered spectral bands proposal for a new assessment methodology for an adaptive demonstrator
 - (4) laboratory testing, to determine the properties of the camouflage materials and coatings. Research should be performed on:
 - mechanical and thermal properties;
 - resistance to external factors (water, dust, fire, weather);
 - chemical resistance to e.g., lubricants, disinfectants;
 - spectral characteristics and measurements, and,
 - evaluation of gloss and contrast.
 - (5) Development of a concept of a self-adapting closed loop:
 - collection of surrounding environment flux in the considered spectral bands
 - specification and assessment of different technical possibilities;
 - selection of suitable feedback sensors in different spectral bands, and;
 - analysis of a digital based control unit with an interface to allow integration into an overall system concept.
 - (6) definition of the energy budget for each active adaptive camouflage technique considered, including analysis and evaluation of alternative power sources for generating and storing electricity and creating conditions for an autonomous mode of using electricity.
 - (7) Technology demonstration on a military platform or soldier using standard-like surrogate targets; as for example a human body dummy and vehicle dummy.
- Integrating knowledge
 - (1) establishment of a concept of combining and integrating different, active and passive adaptive techniques in a mixed structure (layers, mosaic), including but not limited to ECPs, LEDs, NIR-diodes and flexible electrochromic display, optical fibres and new fibres based on dual technologies, transparent paintings, digital printing for active and passive camouflage, cooling elements, layers with spacers, etc. Biologically inspired materials and structures could be considered as well;
 - (2) analysis of the technical feasibility, requirement specification, trade-offs and concept definition for an operational use case.

- Studies
 - (1) study of novel materials with potential to improve signature management beyond state-of-the-art;
 - (2) study on the development of easy to scale-up technologies of elastic elements, as well as production of textile, preferably recyclable materials, with specific camouflage properties;
 - (3) analysis of industrialization and technology maturation needs at EU level;
 - (4) analysis of the disruptive potential of specific solutions for adaptive camouflage.
- Design
 - (1) design and testing of the surface structure;
 - (2) design and build a demonstrator, performing measurements at different environmental conditions in different spectral bands, compare to different background signatures and intensities;
 - (3) construction of a unified technology demonstrator;
 - (4) performance verification of the technology demonstrator in laboratory-conditions as well as under field conditions.

Functional requirements

It is essential that the research activities generate new or improved camouflage capability according to requirements generated from the operational needs of the Member States and Norway military forces.

Final adaptation to physical requirements regarding e.g., mobility, size, weight, power consumption, platform integration, and general robustness is not excluded, but more suited for a development program phase. Nevertheless, the proposals should include considerations on how the technology development can be driven with these parameters in mind.

The proposals should meet the following functional requirements:

- camouflage systems for both soldiers and military platforms should be considered;
- the camouflage should be functional in the different spectral bands listed in footnote 16;
- the camouflage should be able to be integrated with the platform or soldier C4I technology and should require power source appropriate for the platform or the soldiers' energy supply;
- power consumption should be minimized because it is critical for many missions (e.g., for all unmounted scenarios). The active camouflage for soldier should possess sufficient electrical independence: reduced power consumption in case of electronic components, as well as a self-recharging system. For vehicle applications power consumption is not as critical;

- all proposed solutions should clearly indicate required power, voltage and current, in order to be able to compare the proposals to the generators or batteries of existing vehicles and batteries of dismounted personnel;
- the active camouflage should be equipped with user protection system preventing from risk of electric shock;
- the most crucial aspect is the compatibility of all the spectral protection measures into a unified compact multitool, applicable for single soldier and military systems;
- the active camouflage control system should automatically generate suitable camouflage patterns ensuring low level of detectability efficiently;
- the active camouflage system must have a cyber security protection to prevent targeting by enemy systems;
- different optical intensities, colours and patterns should be generated;
- different weather conditions (summer, winter, sunshine, night, rain) and different background scenarios (woodland, desert, urban) should be taken into account;
- the active camouflage material should demonstrate good mechanical properties, such as strength, low weight, compact structure and ease of use, allowing easy transportation and handling;
- the working principle of the control loop and the feedback signals should be defined;
- the possibility to integrate into an overall military system concept for different carriers with compatibility to other equipment and boundary conditions should be considered;
- for the technology demonstration on a human body, a standard-like dummy target could be considered;
- for the technology demonstration on a vehicle a standard-like target such as the (EDA) STANDCAM could be considered;
- current available assets, as the European Terrain Database (EDA), could be exploited to assess camouflage effectiveness of soldiers and military platforms as well as the effectiveness of sensors in different terrains.

The functional requirements also include the optical properties of an adaptive shield (flexible or rigid) with an arrangement of different adaptive elements in different spectral bands also possessing radar protection. Properties to cover should be (if applicable):

- selection of materials with good performance in terms of their durability, usability, resilience, and low undesirable impact on other spectral ranges;
- increased camouflage effectiveness in spectral bands listed in footnote 16;
- spatial distribution of the emitted light and reflected environmental light, described by the BRDF (Bidirectional Reflectance Distribution Function) should be considered;
- polarization signature should be considered;
- speed of the adaptive change;

- properties of the closed feedback-loop with respect to different sensors, digital hardware, control concept, accuracy and speed.

Expected impact

- Contribute to closing the technical gaps directly related with the capabilities described in the CDP for the priority “Ground Combat Capabilities”:
- upgrade, modernize and develop Land platforms to adapt to operational environment;
- upgrade of current and development of next generation armoured platforms.
- Enhance protection of forces with feasible solutions and improve of Land mobility.
- Improvement in military tactics and missions.
- Enabling of mission profiles that cannot be executed using conventional non-adaptive camouflage.
- New materials, new sensing techniques and new production techniques will create a renewed and variety of options in the world of “seek and hide” by combining selected Visible, IR and radar camouflage combinations, according with specific mission needs and requirements.
- Improve individual soldier protection.
- Decreases exposure to the enemy’s actions, decreasing the number of combat casualties.

2.2.2. EDF-2022-LS-RA-DIS-EAD: Electromagnetic artillery demonstrator

- **Indicative budget:**

The Union is considering a contribution of up to EUR 15 000 000 for this topic under the call EDF-2022-LS-RA-DIS

- **Number of actions to be funded:** Several actions, addressing different solutions, may be funded for this topic

Objectives

The combination of electromagnetic artillery guns with smart ammunition can provide long-range precision strikes, as well as increased air defence and anti-surface warfare capabilities. Such combination is expected to improve the effectiveness and the protection of future European land and naval systems. Electromagnetic guns might provide a drastic superiority over conventional guns due to its hypersonic muzzle velocities, while guided projectiles will provide higher accuracy and precision. This topic complements ongoing projects, in particular following the 2019 PADR call on emerging technologies for defence.

General objective

Long-range effects are a substantial contributor to capability priorities concerning sea surface superiority and ground combat capabilities to maintain indirect / over-the-horizon fire support over large distances for precision strikes against a brought spectrum of targets. Physical limits of existing artillery systems in highly agile symmetric warfare scenarios call for exploring radical game-changing concepts, that combine increased performance and safety on the

battlefield and that cannot be achieved with conventional (chemical) propellants and launchers. These will allow European technology and industry to remain at the leading-edge, contributing to technological supremacy and European Strategic Autonomy in the defence sector.

Specific objective

Considering the requirements for enhanced precision and extended range of ammunition, while seeking affordable costs, Electromagnetic accelerators, or guns (EMG) represent a disruptive technology to launch projectiles over extremely long distance ($> 200 \text{ km}^{18}$) and muzzle velocities. Thus, an EMG system is a promising option to fill the gap between conventional artillery (cost effective but limited to 70 km^{19} range) and missiles (long-range but expensive and therefore limited to high-level targets).

An EMG system consists of the three major components, the accelerator or electromagnetic gun itself, the conversion and storage unit, and the projectile. These components present different technology maturity levels and affect the total system efficiency. Two basic concepts have been investigated for military applications, the railgun (EMRG) and the coilgun²⁰ (EMCG).

In Europe, the technological maturity of the EMG systems system is currently located in the range between TRL 3 and TRL 4, which means that the experimental proof of concept is done and the technology is being validated in a laboratory environment.

Feeding the EMG with a large amount of energy in a very short time is a challenge. The electric pulsed power, that is needed to supply the EMG, requires storage space close to the gun barrel. Electrical storage is under the constraint of at least two parameters: the first parameter is the volume needed for the hardware (related to the energy density of the storage, that is to say, to the storage weight); the second parameter is the capability of the storage to deliver the energy in a very short duration.

The projectile and the electromagnetic launcher have to be co-developed. In the case that electronic parts and other electromagnetically sensitive parts has to be integrated into the projectile magnetic shielding has to be taken into account for the system-specific projectile design. EMG are most frequently working with square calibres. Rectangular or round calibres can also be used, which are more challenging because of the need for sabots or laborious constructive measures This means that a large variety of projectile shapes are possible and offer the opportunity to develop out-of-the-box aerodynamic concepts.

A large calibre weapon with an extremely high muzzle velocity, achieved by electromagnetic propulsion (hypervelocity regime), has major benefits like longer ranges and shorter time-to-target, compared to conventional artillery systems or missiles.

However, developing a large calibre electromagnetic gun is an ambitious goal that will require time to achieve. An intermediate step is required. Besides, considering the emergence of new air threats such as swarms of drones or hypersonic missiles, novel capabilities for air defence missions will be key assets. This is why a medium calibre electromagnetic gun that

¹⁸ According to the research activities conducted in the last years, EMRG artillery may achieve 200 km distance to target in the case of long-range naval applications.

¹⁹ Artillery systems range is today of 40km up to 70km, in case of using precision guided munitions.

²⁰ sometimes also referred to as Gauss-gun.

can be used for air defence and anti-surface warfare is seen as an important goal and also as a milestone in the global roadmap for the development of electromagnetic guns.

Taking into consideration that the electromagnetic gun will be integrated in a naval or land platform, the size and weight of the different components (e.g., components for conversion and storage of energy) are considered a challenge, which needs to be addressed.

Scope and types of activities

Scope

The objective of the topic is to solve the current technical challenges and increase the maturity of the critical components required to develop a medium calibre electromagnetic artillery system.

The focus is set on the following tasks:

- A. Requirement analysis and system specifications of a medium calibre electromagnetic gun dedicated to air defence (primary mission) and anti-surface warfare (secondary mission);
- B. Improved design and development of the critical system components, namely (1) the electromagnetic gun, (2) the pulsed power supply and (3) the hypervelocity projectile, according to the overall system specifications;
- C. Assessment of the components at laboratory level (minimum TRL 4), including their performance validation and the feasibility of their integration at system level.

The priority of this call is to work on the critical components and to make progress on their maturity (B and C), especially for the pulsed power supply.

The whole system development and demonstration (TRL \geq 6) is beyond the scope of the current topic.

Types of activities

The following types of activities are eligible for this topic:

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)	Yes (mandatory)
(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 (mandatory)
(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 design has been developed, including partial tests for risk reduction in an	Yes (mandatory)

Types of activities (art 10(3) EDF Regulation)		Eligible?
	industrial or representative environment	
(e)	System prototyping of a defence product, tangible or intangible component or technology (prototype)	No
(f)	Testing of a defence product, tangible or intangible component or technology	No
(g)	Qualification of a defence product, tangible or intangible component or technology	No
(h)	Certification of a defence product, tangible or intangible component or technology	No
(i)	Development of technologies or assets increasing efficiency across the life cycle of defence products and technologies	No

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

- Definition of the operational requirements of the artillery system: in-depth analysis of the use case scenarios for the following missions:
 - o Primary mission: air defence operations, in particular anti-missile warfare and C-RAM (Counter-Rocket, Artillery, Mortar);
 - o Secondary mission: anti-surface warfare.
- System analysis and specification of an electromagnetic artillery system that complies with the physical and functional integration on military platforms comprising a medium calibre electromagnetic gun a pulsed power supply and hypervelocity projectiles to meet the operational requirements.
- Design of a modular inductive power supply based on XRAM technology, development and test of two modules: the focus is set on size, weight and performance parameters.
- Design of a modular power supply, development and test of two modules (the focus is set on size, weight and performance parameters).
- For power supply technologies: comparing of the two modules and demonstration of the feasibility of modules integration at system level to meet the full system specifications.
- Design, development and test of a medium calibre EMG:
 - o Electrical and mechanical architecture;
 - o Reduction of the gun wear to increase the bore life;
 - o Concept for the EMG loading system according to the firing rate.

- Design, development and test of the sabot and the armature required to accelerate and guide the projectile along the gun bore, search for low-density/high-performance structure to reduce the parasitic mass.
- Design, development and test at short range of instrumented hypervelocity projectiles:
 - o Aerodynamic design: low-drag and heat-resistant aerodynamic architecture;
 - o Investigation of lethality mechanism: kinetic penetrator or airburst/fragmentation warhead;
 - o Hardening of the projectile structure with respect to acceleration, heat and electromagnetic constraints, search for low-density/high-performance structure to optimize space for embedded components such as fuse, explosive, pre-formatted fragment, course control actuators, etc.;
 - o Investigation of course correction devices and GNC (Guidance, Navigation and Control) devices.

Functional requirements

The proposals should meet the following functional requirements:

- Medium calibre electromagnetic artillery system:
 - o Primary mission: air defence, in particular anti-missile warfare and C-RAM;
 - o Secondary mission: anti-surface warfare.
- The system should operate with both naval and ground forces.
- Medium calibre electromagnetic gun:
 - o Total launched mass: from 3 kg to 5 kg (to be refined during the system analysis phase);
 - o Muzzle velocity ≥ 2000 m/s.
- Pulsed power supply:
 - o Energy density ≥ 1 MJ/m³;
 - o Modular design: development of two modules, to demonstrate that the upscaling capability meet the full system specifications.
- Medium calibre hypervelocity projectile:
 - o Low-drag and heat-resistant aerodynamic profile;
 - o Lethality mechanism: kinetic penetrator or airburst/fragmentation warhead;
 - o Mission-specific fuse, explosive, course correction or GNC capabilities.

Expected impact

- Technologies identified in this topic directly contribute to the development of “next generation precision strike capabilities”, under the CDP priority “Ground Combat Capabilities”.

- They also contribute to “Naval Manoeuvrability” CDP priority, by providing disruptive technologies for surface superiority and power projection from sea.
- Concerning CDP “Air Superiority”, EMG technology will enhance “Suppression of Enemy Air Defence (SEAD)” capability, in order to mitigate adversary Air Defence systems.
- These technologies are further in compliance with European Defence Agency (EDA)’s Overarching Strategic Research Agenda (OSRA) results.
- Contribution to the defence and security interests of the EU, its Member States and Norway:
 - o Contribution to EU strategic autonomy;
 - o Increased protection of critical assets as well as ground and naval units;
 - o Reduced life-cycle cost compared to current systems.
- Contribution to European technological sovereignty:
 - o Reinforcement of innovation capabilities through the investigation of new and disruptive concepts and technologies;
 - o Strengthening of the EU’s Defence Technological and Industrial Base (EDTIB).

2.2.3. EDF-2022-LS-RA-DIS-NT: Non-thematic research actions targeting disruptive technologies for defence

- **Indicative budget:** the Union is considering a contribution of up to EUR 10 000 000 for this topic under the call EDF-2022-LS-RA-DIS.
- **Number of actions to be funded:** several actions, addressing different solutions, may be funded for this topic.
- **Range of financial contribution of the Union per proposal:** the requested funding should match the ambition of the proposed action and be duly justified. In any case, the requested funding should not exceed EUR 4 000 000.

Objectives

The specific challenge is to lay the foundations for radically new future technologies of any kind with unexpected impact that aims to bring radical technological superiority over potential adversaries. This topic also encourages the driving role of new actors in defence research and innovation, including excellent researchers, ambitious high-tech SMEs and visionary research centres of big companies, universities or research and technology organisations.

Scope and types of activities

Scope

Proposals are sought for cutting-edge, high-risk/high-impact research leading to game-changing impact in a defence context. They must have the following essential characteristics:

- a disruptive impact in a defence context: Proposals need to clearly address how the proposed solutions would create a disruptive effect when integrated in a realistic military operation;
- radical vision: Proposals must address a clear and radical vision, enabled by a new technology concept that challenges current paradigms. In particular, research to advance on the roadmap of a well-established technological paradigm, even if high-risk, will not be funded;
- breakthrough technological target: Proposals must target novel and ambitious scientific or technological breakthroughs that can be experimentally assessed, and the suitability of the concept for new defence applications must be duly demonstrated. Basic research without a clear technological objective targeting defence applications will not be funded.

The inherently high risks of the research proposed must be mitigated by a flexible methodology to deal with the considerable science-and-technology uncertainties and for choosing alternative directions and options.

Proposals should include clear descriptions of the proposed criteria to assess work package completion.

Types of activities

The following types of activities are eligible for this topic:

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)	Yes (mandatory)
(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 design has been developed, including partial tests for risk reduction in an industrial or representative environment	Yes (optional)
(e)	System prototyping of a defence product, tangible or intangible component or technology	No
(f)	Testing of a defence product, tangible or intangible component or technology	No

(g)	Qualification of a defence product, tangible or intangible component or technology	No
(h)	Certification of a defence product, tangible or intangible component or technology	No
(i)	Development of technologies or assets increasing efficiency across the life cycle of defence products and technologies	No

Functional requirements

This call is open to any technology with a high disruption potential. Proposals should describe the targeted functionalities and the foreseen means to measure progress toward the achievements of these functionalities.

Expected impact

- Scientific and technological contributions to the foundation of a future technology with disruptive applications in the area of defence.
- Enhanced innovation capacity of the European Defence industry by identifying and exploring ground-breaking concepts and approaches or by applying technologies and concepts previously not applied in the defence sector.
- Enhanced competitiveness of the European defence industry and creation of new defence markets.
- Enhanced defence research and innovation capacity across Europe by involvement of actors that can make a difference in the future such as excellent researchers, ambitious high-tech SMEs or visionary departments of big companies, research centres and universities.

2.3. Call EDF-2022-LS-RA-CHALLENGE

- **Targeted type of actions:** Research actions (technological challenge)
- **Form of funding:** Lump sum grants following the call for proposals
- **Targeted type of applicants:** Any eligible consortium as defined in Articles 9 and 10(4) of the EDF Regulation
- **Indicative budget for the call:** The Union is considering a contribution of up to EUR 25 000 000 to support the following 2 call topics:

2.3.1. EDF-2022-LS-RA-CHALLENGE-DIGIT-HTDP: Unmanned ground and aerial systems for hidden threats detection – Participation to a technological challenge

- **Indicative budget:** the Union is considering a contribution of up to EUR 20 000 000 for this topic under the call EDF-2022-LS-RA-CHALLENGE.
- **Range of financial contribution of the Union per proposal:** the requested funding should not exceed EUR 5 000 000.

- **Number of actions to be funded:** Several actions related to the participation in the challenge and addressing different solutions may be funded for this topic.

Objectives

Improvised explosive devices (IEDs) and landmines are a significant threat to military personnel, civilians and equipment, and a major cause of casualties for European forces during operations. Countering these hidden threats is essential to protect soldiers, reduce loss of equipment, secure critical logistic activities, improve mobility and freedom to act by increasing the security of operation areas, and more generally enhance operational efficiency. Furthermore, in a hybrid warfare context, these threats are increasingly used against civilian populations. In particular, they have the potential to severely disrupt both military and civilian supply chains, damage critical infrastructures and affect strategic lines of communication.

Detecting these hidden threats is a first essential step to counter them. Since they are by design difficult to detect for humans, automatic detection technologies can play an important role. However, the task is intrinsically difficult, and the performance of existing technologies is still far from answering the needs. Scenarios classically encountered by armed forces in past missions such as route clearance already represent a challenge. In addition, IEDs are increasingly used in urban scenarios where the detection is even more difficult, especially if multiple IEDs emplacements are used. There is a need to enhance detection technologies, especially for scenarios where single detection devices are not sufficient and the use of distributed sensors is deemed useful. There is also a need to determine their type (e.g., how they are triggered), in particular to ease their neutralisation (rendering safe, disabling or destroying).

While the above issues have been the subject of much research over many years, progress is hindered by the lack of standardised benchmarks, and there is a need to evaluate the performances of integrated functional demonstrators in an objective and comparable manner, using representative testing environments and well-defined metrics.

Overall progress in IED and landmine detection and characterisation can be driven by progress along several lines:

- Physics-based sensors enhancement;
- Collection of representative data, combined with various artificial intelligence (AI) techniques, e.g., computer vision for object detection and localisation;
- Use of various sensors borne by a fleet of unmanned ground and aerial systems, combined with information fusion techniques;
- Better exploitation of limited amounts of data and use of models that are easier to adapt to new environments (through innovative AI techniques such as learning methods requiring less supervision from expert developers, transfer learning...);
- Multidisciplinary cooperation between the hardware sensors and AI communities.

Scope and types of activities

Scope

Proposals should address technological solutions to detect and characterise IEDs and landmines in complex environments, using a combination of advanced sensors, information fusion from these sensors, and unmanned ground and aerial systems to extend the detection capabilities. These solutions should be evaluable through the testing environment set up in the framework of the technological challenge.

Proposals should include clear descriptions of criteria to assess work package completion. Criteria should include the participation to the test campaigns organised in the framework of the technological challenge, the delivery of sensor data collected during the field tests, and the delivery of descriptions of the systems submitted to the tests.

Types of activities

The following types of activities are eligible for this topic:

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)	Yes (mandatory)
(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 design has been developed, including partial tests for risk reduction in an industrial or representative environment	Yes (optional)
(e)	System prototyping of a defence product, tangible or intangible component or technology (prototype)	No
(f)	Testing of a defence product, tangible or intangible component or technology	No
(g)	Qualification of a defence product, tangible or intangible component or technology	No
(h)	Certification of a defence product, tangible or intangible component or technology	No
(i)	Development of technologies or assets increasing efficiency across the life cycle of defence products and technologies	No

The proposals must address in particular the following as part of the mandatory activities:

- Research on new approaches and technologies for hidden threat detection and characterisation
- Participation to the evaluation campaigns organised in the framework of the technological challenge, including
 - o Contribution to the exchanges with other stakeholders on the evaluation plans
 - o Submission of the systems to experimental performance measurements during the field and online test campaigns managed by the challenge organisers
 - o Collection and sharing of data
 - o Participation to debriefing workshops

Functional requirements

The proposed solutions should fulfil the following requirements:

- Ability to go through a zone with IEDs or landmines while minimizing the risk of damage
- Ability to detect and map IEDs and landmines in a given area, with maximum accuracy
- Ability to characterise IEDs and landmines, with maximum accuracy

The performances for these abilities should be measurable through the test campaign conducted in the framework of the technological challenge, using protocols and metrics based on those described in the preliminary evaluation plan provided as part of the call documents. Details about how the proposed approaches and systems will address the tasks outlined in the preliminary evaluation plan should be described in the proposals.

Systems should be able to record the data acquired through their sensors, in order to enable reproduction of experiments in a software environment. The types of data that could be shared with other teams should be described in the proposals.

While much flexibility is left concerning the system configuration for the challenge, systems should be designed to experiment operationally relevant solutions.

Expected impact

The expected impacts are:

- Enhanced clarity on performances of equipment for IED and landmine detection and characterisation
- Availability of databases to further develop and test equipment
- Enhanced soldier protection and increased survivability, through reduced risk for lethal or damaging incidents
- Enhanced freedom of action
- Reduced risks of disruption of strategic infrastructures

2.3.2. EDF-2022-LS-RA-CHALLENGE-DIGIT-HTDO: Unmanned ground and aerial systems for hidden threats detection – Organisation of a technological challenge

- **Indicative budget for the call:** The Union is considering a contribution of up to EUR 5 000 000 for this topic under the call EDF-2022-CHALLENGE
- **Number of actions to be funded:** Up to one action may be funded for this topic

Objectives

IED and landmine detection has been a research topic for many years. However, progress is hindered by the lack of standardised benchmarks. There is a need to rely on representative testing environments enabling an objective and comparable evaluation of developed systems.

Furthermore, field tests cannot be repeated at will and are not perfectly reproducible, especially for detection systems that involve artificial intelligence. Online tests of software components, for which measurements are easily reproducible and which enable short development cycles, should therefore also be organised. Since little data is readily available, data for online tests need to be collected during field tests organised previously during the challenge. This combination of field tests and online tests is needed to steer fast progress toward operational goals.

Scope and types of activities

Scope

Proposals should address the organisation of a technological challenge on IED and landmine detection based on the preliminary evaluation plan provided as part of the call documents. This includes the collection of data recorded by the participating teams during field tests, the annotation of this data and the sharing of the resulting databases.

Proposals should include clear descriptions of criteria to assess work package completion. Criteria should include the production of detailed evaluation plans agreed upon by all stakeholders, the production of the annotated databases needed for the evaluations, the production of measurements for all systems submitted to the tests by the participating teams following these plans, and the organisation of the needed events.

Types of activities

The following types of activities are eligible for this topic:

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)	Yes (optional)
(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 (mandatory)

Types of activities (art 10(3) EDF Regulation)		Eligible?
(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 design has been developed, including partial tests for risk reduction in an industrial or representative environment	Yes (optional)
(e)	System prototyping of a defence product, tangible or intangible component or technology (prototype)	No
(f)	Testing of a defence product, tangible or intangible component or technology	No
(g)	Qualification of a defence product, tangible or intangible component or technology	No
(h)	Certification of a defence product, tangible or intangible component or technology	No
(i)	Development of technologies or assets increasing efficiency across the life cycle of defence products and technologies	No

The proposals must address in particular the following as part of the mandatory activities:

- Setting up of the hardware and software infrastructures for testing hidden threat detection and characterisation technologies in the framework of the technological challenge
- Collection of sensor data from the participating teams, annotation of the data with ground truth information, and quality assessment, distribution and curation of databases
- Organisation of the evaluation campaigns, and in particular
 - o Coordination of the exchanges with other stakeholders on the evaluation plans and elaboration of these plans
 - o Management of the experimental hardware and software test campaigns and of the objective measurements of the performances of the systems submitted to the tests by the participating teams according to the protocols and metrics described in the evaluation plans
 - o Organisation of the debriefing workshops

Functional requirements

The proposed solutions should enable to measure the performances of the tested systems according to detailed evaluation plans based on the preliminary evaluation plan provided as part of the call documents. Key aspects of the foreseen detailed evaluation plans and

associated data management should be described in the proposals. Proposals should in particular describe:

- scenarios, nature and size of test ranges, and environmental conditions,
- types of devices, concealment, attack geography,
- nature and volume of data annotation,
- the framework for trusted sharing of data,
- the detailed planning of the test campaigns, including how runs can be organised in parallel on several test ranges,
- evaluation procedures (rules and tools to implement the metrics) and significance tests performed on measurements.

The testing environment should be able to accommodate for up to six participating teams.

During the challenge, drafts of the detailed evaluation plans should be submitted for discussion to the participating teams and to any stakeholder designated by the funding authority, early enough to take into account the feedback for the actual evaluation campaigns. Any evolution of the evaluation plans should take into account several factors: technical possibilities and cost, scientific relevance of the measurement, and representativeness of the metrics and protocols with respect to military needs. The justification of any change that is not subject to a consensus should be documented.

Expected impact

The expected impacts are

- Enhanced metrics and protocols to measure progress of R&D on IED and landmine detection and characterisation
- Standardisation of combined online and field testing for IED and landmine detection and characterisation
- Availability of databases to further develop and test equipment
- Enhanced clarity of system performances for all stakeholders, including system developers, funders and users
- Enhanced community building for the topic.

2.4. Call EDF-2022-DA

- **Targeted type of actions:** development actions.
- **Form of funding:** actual costs grants following the call for proposals.
- **Targeted type of applicants:** any eligible consortium as defined in Articles 9 and 10(4) of the EDF Regulation.
- **Indicative budget for the call:** the Union is considering a contribution of EUR 510 000 000 to support the following 12 call topics:

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

- **Indicative budget:** the Union is considering a contribution of up to EUR 30 000 000 for this topic under the call EDF-2022-DA.
- **Number of actions to be funded:** up to one action may be funded for this topic

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*²¹.

Types of activities

The following types of activities are eligible for this topic:

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 design has been developed, including partial tests for risk reduction in an industrial or representative environment	Yes (mandatory)
(e)	System prototyping of a defence product, tangible or intangible component or technology (prototype)	Yes (optional)
(f)	Testing of a defence product, tangible or intangible component or technology	Yes (optional)
(g)	Qualification of a defence product, tangible or intangible component or technology	Yes (optional)
(h)	Certification of a defence product, tangible or intangible component or technology	Yes

²¹ <https://ec.europa.eu/info/funding-tenders/opportunities/portal/screen/opportunities/topic-details/edidp-esc2s-2019>

Types of activities (art 10(3) EDF Regulation)		Eligible?
		(optional)
(i)	Development of technologies or assets increasing efficiency across the life cycle of defence products and technologies	Yes (optional)

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.

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.
- ORBAT²² 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),

²² Order of battle report

Recognized Engineer Picture (RENGGP), Recognized Cyber Picture (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.

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

- **Indicative budget:**

The Union is considering a contribution of up to EUR 20 000 000 for this topic under the call EDF-2022-DA.

- **Number of actions to be funded:** Up to one action may be funded for this topic

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, HVAC²³, 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 types of activities are eligible for this topic:

²³ Heating Ventilation and Air Conditioning

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 design has been developed, including partial tests for risk reduction in an industrial or representative environment	Yes (mandatory)
(e)	System prototyping of a defence product, tangible or intangible component or technology (prototype)	Yes (mandatory)
(f)	Testing of a defence product, tangible or intangible component or technology	Yes (mandatory)
(g)	Qualification of a defence product, tangible or intangible component or technology	Yes (optional)
(h)	Certification 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.
- 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.

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

- **Indicative budget:** the Union is considering a contribution of up to EUR 33 000 000 for this topic under the call EDF-2022-DA.
- **Number of actions to be funded:** Several actions, addressing different solutions, may be funded for this topic

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 Warfare²⁴. 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

²⁴ https://www.nato.int/nato_static_fl2014/assets/pdf/2020/5/pdf/2005-deeportal4-information-warfare.pdf

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 types of activities are eligible for this topic:

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 design has been developed, including partial tests for risk reduction in an industrial or representative environment	Yes (mandatory)
(e)	System prototyping of a defence product, tangible or intangible component or technology (prototype)	Yes (mandatory)
(f)	Testing of a defence product, tangible or intangible component or technology	Yes (optional)
(g)	Qualification of a defence product, tangible or intangible component or technology	Yes (optional)
(h)	Certification of a defence product, tangible or intangible component or technology	Yes (optional)

Types of activities (art 10(3) EDF Regulation)		Eligible?
(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:
 - o Attacks against deployed forces in operations;
 - o 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.

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

- **Indicative budget:**

The Union is considering a contribution of up to EUR 27 000 000 for this topic under the call EDF-2022-DA.

- **Number of actions to be funded:** Several actions, addressing different solutions, may be funded for this topic for this topic

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 types of activities are eligible for this topic:

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 design has been developed, including partial tests for risk reduction in an industrial or representative environment	Yes (mandatory)
(e)	System prototyping of a defence product, tangible or intangible component or technology (prototype)	Yes (optional)
(f)	Testing of a defence product, tangible or intangible component or technology	Yes (optional)
(g)	Qualification of a defence product, tangible or intangible component or technology	Yes (optional)
(h)	Certification of a defence product, tangible or intangible component or technology	Yes (optional)

Types of activities (art 10(3) EDF Regulation)		Eligible?
(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 HW²⁵ & SW²⁶ 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.

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;

²⁵ Hardware
²⁶ Software

- 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.

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

- **Indicative budget:**

The Union is considering a contribution of up to EUR 40 000 000 for this topic under the call EDF-2022-DA.

- **Number of actions to be funded:** Up to one action may be funded for this topic

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, SAR²⁷ and SIGINT²⁸ 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.

²⁷ Synthetic aperture radar.

²⁸ 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)*²⁹.

²⁹ <https://ec.europa.eu/info/funding-tenders/opportunities/portal/screen/opportunities/topic-details/edidp-msc-mfc-2020>

Types of activities

The following types of activities are eligible for this topic:

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 design has been developed, including partial tests for risk reduction in an industrial or representative environment	Yes (mandatory)
(e)	System prototyping 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 of a defence product, tangible or intangible component or technology	Yes (optional)
(h)	Certification 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
 - o 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 AI³⁰-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
 - the development of a prototype for selected payloads and/or subsystems;
- Testing and qualification

³⁰ Artificial intelligence

- 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.

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

- **Indicative budget:**

The Union is considering a contribution of up to EUR 90 000 000 for this topic under the call EDF-2022-DA.

- **Number of actions to be funded:** Up to one action may be funded for this topic

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 challenge

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 types of activities are eligible for this topic:

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 design has been developed, including partial tests for risk reduction in an industrial or representative environment	Yes (mandatory)

(e)	System prototyping 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 of a defence product, tangible or intangible component or technology	Yes (optional)
(h)	Certification 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 C2³¹ (*e.g.*, NATO, EU and national C2, radars, BMD and SSA³² 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;

³¹ Command and control

³² Space situational awareness

- update of programmatic elements (e.g., costs, planning, risks, cooperation scheme) for the development of a European SBMEW capability.

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.

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

- **Indicative budget:** The Union is considering a contribution of up to EUR 20 000 000 for this topic under the call EDF-2022-DA
- **Number of actions to be funded:** Several actions, addressing different solutions, may be funded for this topic

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 life 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 types of activities are eligible for this topic:

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)

Types of activities (art 10(3) EDF Regulation)		Eligible?
(d)	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, including partial tests for risk reduction in an industrial or representative environment	Yes (mandatory)
(e)	System prototyping of a defence product, tangible or intangible component or technology (prototype)	Yes (mandatory)
(f)	Testing of a defence product, tangible or intangible component or technology	Yes (mandatory)
(g)	Qualification of a defence product, tangible or intangible component or technology	Yes (optional)
(h)	Certification 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:
 - o signature reduction function
 - o ballistic and protective functions
 - o textile mechanical properties
 - o washability or other maintenance and durability
 - o 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:
 - o active or passive regulation of body temperature in case of extreme weather conditions (hot or cold)
 - o 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:
 - o Monitoring of various physiological data for dedicated use cases.
 - o Drug delivery and/or emergency care to act on blood loss and other traumas, using data collected through monitoring
 - o Acquire localization data
 - o protection of medical collected data all along the process to comply with confidentiality
 - o compliance of processing and utilization of medical data with ethical rules
 - o protection of the data collected for environment and equipment monitoring
 - o data formats corresponding to relevant standards and connection with relevant interfaces.
- In the field of Energy management:
 - o 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:
 - o 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

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

- **Indicative budget:**

The Union is considering a contribution of up to EUR 40 000 000 for this topic under the call EDF-2022-DA

- **Number of actions to be funded:** Up to one action may be funded for this topic

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*³³.

Types of activities

The following types of activities are eligible for this topic:

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	No

³³ <https://ec.europa.eu/info/funding-tenders/opportunities/portal/screen/opportunities/topic-details/edidp-acc-aeac-2019>

Types of activities (art 10(3) EDF Regulation)		Eligible?
	of defence (generating knowledge)	
(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 design has been developed, including partial tests for risk reduction in an industrial or representative environment	Yes (mandatory)
(e)	System prototyping of a defence product, tangible or intangible component or technology (prototype)	Yes (mandatory)
(f)	Testing of a defence product, tangible or intangible component or technology	Yes (mandatory)
(g)	Qualification of a defence product, tangible or intangible component or technology	Yes (optional)
(h)	Certification 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:
 - o 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.
 - 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:
 - o Stand-In jammer (SIJ): Small sizes and in swarms coordinated UAVs or ALD (decoys).
 - o Escort jammer: Installed on a platform which guides or is part of an attacking A/C strike.
 - o 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:

- o Development in near real time of EOB
- o Analysis and Mission Planning and restitution (off-line)
- o Distributed and coordinated approach to the mission
- o Multi-platform cooperative jamming
- o 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 led 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.

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

- **Indicative budget:**

The Union is considering a contribution of up to EUR 50 000 000 for this topic under the call EDF-2022-DA

- **Number of actions to be funded:** Several actions, addressing different solutions, may be funded for this topic

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 UAV³⁴s 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 CBRN³⁵ 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 solutions³⁶ 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;
- 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;

³⁴ Unmanned Aerial Vehicles

³⁵ Chemical, Biological, Radiological and Nuclear

³⁶ Taking into account the possible latency and limited bandwidth of the communication network to perform collaborative service orchestration.

- 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 types of activities are eligible for this topic:

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

Types of activities (art 10(3) EDF Regulation)		Eligible?
(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 design has been developed, including partial tests for risk reduction in an industrial or representative environment	Yes (mandatory)
(e)	System prototyping of a defence product, tangible or intangible component or technology (prototype)	Yes (mandatory)
(f)	Testing of a defence product, tangible or intangible component or technology	Yes (optional)
(g)	Qualification of a defence product, tangible or intangible component or technology	Yes (optional)
(h)	Certification 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 typology, same grid references, etc.) seems to be a necessity for data exploitation and will facilitate a common understanding of tactical situations
 - o In 2 dimensions;
 - o In 2.5 dimensions;
 - o 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 changer³⁷;
- 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:
 - o Various kinds of sensors (e.g., optronics, warning systems, navigation sensors);
 - o 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.

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.

³⁷ Allowing subsidiarity and data filtering to transfer only the more useful and adequate information within the network

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.

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

- **Indicative budget:**

The Union is considering a contribution of up to EUR 65 000 000 for this topic under the call EDF-2022-DA

- **Number of actions to be funded:** Up to one action may be funded for this topic

Objectives

The goal is to study, design, prototype and test a medium-sized semi-autonomous surface vessel (MSAS) with at least an ISR³⁸ modular mission payload.

³⁸ Intelligence, Surveillance, Reconnaissance

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.

Semi-autonomy should be understood as a primarily option to operate the platform and mission modules remotely. Due to the constraints 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 practice³⁹ 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.

³⁹ 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.

LEVEL 3: Modularity and affordability

Mission dedicated naval assets are typically too expensive and unaffordable for small navies to cover sufficiently broad 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 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 types of activities are eligible for this topic:

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 design has been developed, including partial tests for risk reduction in an industrial or representative environment	Yes (mandatory)
(e)	System prototyping of a defence product, tangible or intangible component or technology (prototype)	Yes (mandatory)
(f)	Testing of a defence product, tangible or intangible component or technology	Yes (mandatory)
(g)	Qualification of a defence product, tangible or intangible component or technology	Yes (optional)
(h)	Certification 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:
 - o Technical feasibility studies must include, at least, the following aspects:
 - core components (e.g., autonomy including COLREG⁴⁰ 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:
 - o System architecture.
 - o Core platform, including ISR module.
 - o Autonomy package.
 - o Control station (equipment needed for remote/autonomous monitoring/control of MSAS).
 - o Secure communication suit (e.g., internal, seashore, sea-sea).
 - o Mission modules and mission modules integration.
- Prototyping:
 - o Core platform with all key components, including ISR module.
 - o Control station (equipment needed for remote/autonomous monitoring/control of Platform).
- Testing:
 - o Components and system integration.
 - o 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.

⁴⁰ Convention on the International Regulations for Preventing Collisions at Sea, 1972

- 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, the selection of propulsion plant and propelling system should consider reaching minimum 20 knots at maximum RPM⁴¹ 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 AI⁴² 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 USVs⁴³ and/or UUVs⁴⁴ and the MSAS operating as a rely-station to extend the operating radius.

(2) Positioning, Guidance, Navigation and Control

- a. Alongside the encrypted (military) GNSS⁴⁵, 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

⁴¹ Revolutions per minute
⁴² Artificial Intelligence
⁴³ Unmanned Surface Vehicle
⁴⁴ Unmanned Underwater Vehicle
⁴⁵ Global Navigation Satellite Systems

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.
- 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's⁴⁶ 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/IR⁴⁷) should be transmitted automatically via secure communications, to the control station. It

⁴⁶ International Maritime Organization

⁴⁷ Electro optical/infrared

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
- 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 C4ISR48 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;

⁴⁸ Command, Control, Communications, Computers, Intelligence, Surveillance and Reconnaissance

- Secure communication systems, gaining access to ship's GNC⁴⁹ 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.
- 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.

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

- **Indicative budget:**

The Union is considering a contribution of up to EUR 65 000 000 for this topic under the call EDF-2022-DA

- **Number of actions to be funded:** Up to one action may be funded for this topic

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),

⁴⁹ Guidance, navigation and control

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 types of activities are eligible for this topic:

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	Yes (optional)

Types of activities (art 10(3) EDF Regulation)		Eligible?
	defence products and technologies (integrating knowledge)	
(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 design has been developed, including partial tests for risk reduction in an industrial or representative environment	Yes (mandatory)
(e)	System prototyping of a defence product, tangible or intangible component or technology (prototype)	Yes (mandatory)
(f)	Testing of a defence product, tangible or intangible component or technology	Yes (mandatory)
(g)	Qualification of a defence product, tangible or intangible component or technology	Yes (optional)
(h)	Certification 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:
 - o The evolutions of the EU protocol/interface standard required for each of the foreseen NCS capability levels 1, 2 and 3.
 - o 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.

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

- **Indicative budget:**

The Union is considering a contribution of up to up to EUR 30 000 000 for this topic under the call EDF-2022-DA

- **Number of actions to be funded:** Up to one action may be funded for this topic

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), C4I⁵⁰ 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, leveraging 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 and development of new and integration of state-of-the-art technologies in training and decision-making using simulation systems.

⁵⁰ Command Control Communication Computer and Information

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 types of activities are eligible for this topic:

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 design has been developed, including partial tests for risk reduction in an industrial or representative environment	Yes (mandatory)

Types of activities (art 10(3) EDF Regulation)		Eligible?
(e)	System prototyping of a defence product, tangible or intangible component or technology (prototype)	Yes (mandatory)
(f)	Testing of a defence product, tangible or intangible component or technology	Yes (optional)
(g)	Qualification of a defence product, tangible or intangible component or technology	Yes (optional)
(h)	Certification 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 prospecting 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&E⁵¹ 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

⁵¹ Concept Development and Experimentation

other standardization organisations (SISO/IEEE/OGC/ISO). (e.g., 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 NMSG⁵² 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).

⁵² NATO Modelling and Simulation Group

- 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 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., WAN⁵³, SATCOM⁵⁴).
- 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

⁵³ Wide Area Network

⁵⁴ SATellite COMmunications

and logistics) with the aim to reach a full integration of them to perform computer-assisted exercises (CAX) and decision-making activities.

(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.

2.5. Call EDF-2022-FPA

- **Targeted type of actions:** To be defined at the level of further specific grants. The call for proposals leads to the signature of a Framework Partnership Agreement covering jointly agreed action plan of activities addressing one category of actions
- **Form of funding:** Framework partnership agreement (FPA) detailing the jointly agreed action plan and the terms and conditions for receiving actual costs grants to implement the actions via specific grant agreements (SGA).
- **Targeted type of applicants:** Any eligible consortium as defined in Articles 9 and 10(4) of the EDF Regulation

2.5.1. EDF-2022-FPA-MCERN-MCM: Framework partnership agreement to support EU defence medical countermeasures Alliance

Introduction

This is a competitive call for proposals for EU **framework partnership agreement (FPA) for grants** in the field of **defence medical countermeasures research and development** under the European Defence Fund (EDF).

This FPA will accommodate annual action grants for the mentioned period; applicants must provide a high-level 4-year action plan and budget for the period of 2023-2026.

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

- Regulation 2018/1046 (EU Financial Regulation);
- Regulation 2021/697 (EDF Regulation).

The call would be launched under the EDF 2022 Work Programme and will be managed by the **European Commission, Directorate-General for Defence Industry and Space (DG DEFIS)**. The outcome of this call is the award and the signature of one Framework Partnership Agreement.

FPAs are long-term cooperation instruments that serve as umbrella for regular or recurrent grants in the same field or area and under a common action plan (or programme of activities). They are prerequisite for being able to apply for these Specific Grant Agreements (SGAs), but do not create any legitimate expectations or entitlement to sign SGAs and get funding. FPA beneficiaries are identified on a basis of a standard evaluation and award procedure and then invited to submit their proposals for grants (invitation to submit applications addressed only to the framework partners). Please note that SGAs can only be signed if the FPA has been signed, and before the end date of the FPA. Applicants are expected to submit their proposal for the first SGA 2023 directly after the signature of the FPA.

Background

Non-traditional CBRN threats are emerging or re-emerging, directly affecting Member States and Norway troops, the Union population and its health, security and prosperity. Member States and Norway defence forces deploy to remote locations around the world. Expeditionary operations become more frequent with smaller forces facing longer and more frequent deployments. At the same time traditional CBRN threats have to be revisited. There is an increasing concern about effects from weapons, agents or courses of action used in symmetric and asymmetric warfare, terrorism as well as indirect and/or unintended threats evolving in hot conflicts, including the use or release of chemical, biological and nuclear weapons and radiological hazards.

Appropriate medical support makes a major contribution to both force protection and morale through prevention of and fight against chemical, biological, radiological and nuclear (CBRN) threats, natural pandemics and diseases, rapid evacuation and treatment of the sick, wounded and injured, and the return to duty of as many individuals as possible.

In line with the **objectives of the European Defence Fund**, this call will support research activities, development activities as well as coordination and networking activities at Union level with and among relevant stakeholders in the policy area of CBRN medical countermeasures and build up the institutional capacity of these stakeholders to contribute actively to the development and implementation of all relevant policies.

This call aims to set up **4-year Framework Partnership Agreements** with European military and civilian research institutes and industry to initiate a core of European research base on military health issues and executed through specific grants covering the activities referred to in article 10.3 of the EDF Regulation.

Objectives - Themes and priorities - Activities that can be funded - Expected impact

Objectives

The framework partnership will support individual troop readiness and total force health protection by developing technologies and products to rapidly identify and respond to biological threats (including natural and genetically modified organism), chemical hazards and attacks, toxins as well as countermeasures regarding radio-nuclear and nuclear threats. Funded actions also focus on the research and development of vaccines and drugs and other antibiological substances (e.g., bacteriophages) against biological agents that may affect a sizable number of the military and/or be used on the battlefield. A subset of the funded actions specifically supports solutions to be used by personnel with minimal medical training, deployable laboratory capabilities even in the low-resource environments typical of many military operations.

The objective of proposals under this call is to update and/or develop medical countermeasures (MCMs) for the armed forces of EU and – wherever applicable - related civil/health protection to respond to the continuously changing and novel health threats posed by CBRN. It thus aims at developing shared capabilities for EU armed forces against CBRN crises, and to treat exposure, pathologies or injuries of significant impact.

This framework partnership will contribute to responding more efficiently to conflicts, crises, or isolated events involving CBRN situations.

Themes and priorities (scope)

To master the evolving threats, the Commission intends to establish a stable and structured partnership with legal entities grouped in a consortium which commit themselves to:

- Create a long-term open, supportive and sustainable cooperation mechanism in Europe amplifying, connecting and strengthening EU (defence) medical research and development capabilities on selected medical threats; and,
- Contribute to the accessibility and availability of medical countermeasures and strengthen their disposability.

Framework partners should focus on innovation, research and development of medical countermeasures against CBRN threats as well as their integration into EU and Member States and Norway health sector, civil protection mechanism and military forces.

Partners may also provide for analysis of the relevance and feasibility of novel MCMs and related technology, further and/or continuous mapping of CBRN MCM capacities across EU, as well as options for ensuring EU's access and availability of MCMs.

MCMs may include clinical testing capabilities or methods, any medicines or medical devices that are aimed at combating CBRN threats. This extends both to countermeasures that prevent or treat the threat. For MCMs to be updated, available and able to respond, this entails a large scope covering innovation, research, development and analysis.

Activities that can be funded (scope)

This partnership will be set up through an FPA, which will enable the **completion of a multiannual action plan** within the context of the agreement.

Applicants are invited to:

- provide clear descriptions of the main activities and implementation methodology;
- describe the contribution and added value of the partnership to the EU policy in the area of this call;
- describe the way in which they use monitoring and/or external evaluations in order to assess their overall performance and the relevance and impact of their outputs

The consortia responding to the call may include military medical commands, research institutes, universities, RTOs, industry, SMEs as well as other organisations that can play a role in the realisation of defence medical countermeasures. The FPA will specify the objectives, the nature of the actions planned, and the procedure for awarding specific grants.

The FPA is expected to contribute to the following outcomes:

- Establish a technology innovation roadmap (multiannual action plan) for linking early-stage capabilities to industry developments.
- Focus on research, innovation and development of defence medical countermeasures against CBRN threats as well as their integration into Member States and Norway military forces, EU health sector and civil protection mechanisms.
- Establish a well-connected network at European level in order to facilitate interoperability in detecting and validating CBRN threats and enlarge capabilities by a consequent cooperation and subsequent division of labour and capacities.
- Stimulate cooperation between European military and civilian research institutes and industry to initiate a core of European research base on military health issues.

Specific grants implemented under the FPA must be in line with the proposed **Action Plan** and may cover one or more of the activities as referred in article 10.3 of the EDF Regulation. For SGAs related to innovation, research and development of MCM products (Drugs and Biologics) the following adapted activities may be covered:

- Generating knowledge: choice of pharmacological target, antigen, or physiological process; target or antibody validation; elucidation of mechanism of action.
- Integrating knowledge: development of industrial production under GMP conditions; demonstration of the stability of MCMs (GMP) in bulk and distributed form (ICH Stability testing of new drug substances and drug products).
- Studies: In vitro assays, in aerosol particles, in vivo proof of concept studies.
- Design: Preclinical trials (DRS, safety, efficacy) on relevant animal models, quality control tests, validation of industrial production process under GMP conditions. Pivotal efficacy studies on animal models as close as possible to humans (authorization under exceptional circumstances).
- Testing: phase I clinical trial with most advanced MCM candidates.
- Qualification: finalization of a dossier for marketing authorization.
- Certification: New drug application (NDA) delivered by the regulatory authority (EMA) or early access program.

Innovative disruptive technologies, like MCMs that limit the development of resistance (e.g., broad-spectrum or highly specific and individualized MCMs), and platforms for local production of MCMs on-demand, may also be covered.

Areas of activities proposed under the Action Plan (scope)

Proposals for the FPA must provide for an **Action Plan** that should cover, but are not limited to, the following areas:

(1) Broad scientific approaches to address general needs

- Research on the properties of and protection from new and emerging CBRN threats
- Developing new technologies for the rapid manufacturing, delivery and distribution of large size medical countermeasures.

(2) Targeted R&D activities that address specific needs

- Development of new generation auto-injectors for antidotes administration.
- Development of technologies, solutions and deployable platforms that integrate, automate, and miniaturize the collection, processing, and analysis of biological and chemical samples.
- Development of novel technologies or measures to treat infections and wounds contaminated by CBR-agents (e.g., sorbent separation mechanism).
- Development on novel Medical Countermeasures against CBRN threats.

(3) High-risk activities with potential pivotal outcomes

- Innovative disruptive methods: Applications or technologies that enables EU to develop novel capabilities such as on demand production of civilian and military-critical materiel and medical countermeasures.
- Development of a mobile, scalable and adaptable European platform for rapid development of medical countermeasures capable of producing relevant numbers of doses against any known or previously unknown CBRN threat within 60 days of identification.
- Development of novel methods to impart near-immediate immunity to an individual using antibodies or generating specific immunity on routes of entry for infection, such as mouth and nose for airborne agents.
- Generation of technologies and scientific knowledge of human physiological responses caused by exposure to any biological or chemical agent.
- Development of new technologies for the simulation of human body response to medical countermeasures against emerging infectious diseases and chemical or biological attacks.

Proposals for FPAs should expand and strengthen the supply chain, aiming for the development of key enabling technologies while improving notions of control of medical countermeasures.

Proposals for FPAs should also develop an IP strategy to protect innovations in the field of medical countermeasures and to provide information about the IPRs that are open to licensing.

Proposals for FPAs should also cover: (i) the collaboration with other initiatives or programmes at regional, national, EU or NATO level and (ii) any additional support they may receive in their activities from relevant national, or regional programmes and initiatives. They should also contribute to spreading excellence across Europe.

Expected impact

The Commission expects the partnership to design and implement **relevant, quality and impactful activities that fit the objectives and priorities** defined in the call. The action plan should clearly demonstrate the organisation's capacity to generate **concrete impacts**.

Applicants are invited to:

- provide clear descriptions of the main activities and implementation methodology;
- describe the contribution and added value of the partnership to the EU policy in the area of this call;
- describe the way in which they use monitoring and external evaluations in order to assess their overall performance and the relevance and impact of their outputs.

In terms of results, the Commission expects the framework partnership to:

- Provide substantial improvements to the CBRN defence domain for Member States and Norway armed forces with consistent CBRN medical protections against a large panel of threats currently not covered by drugs produced within EU;
- Facilitate the development of CBRN defence capabilities that each Member State and associated country, individual government or industry cannot face alone (i.e., a technological platform for the production of medical countermeasures);
- Stimulate cooperation between European military and civilian research institutes and industry to initiate a core of European research base on military health issues,
- Carry out and support coherent projects over the long term and prepare their integration in a global solution (system of systems),
- Strengthen European sovereignty and contribute to the EU strategic autonomy,
- Develop EU autonomous industrial segments.

Even if the main objective of the project is to contribute to the armed forces, its results can also be of interest for the civilian sector.

Available budget

The indicative budget earmarked for grants calls under this framework partnership is **EUR 100 000 000** for the period of 2023-2026.

The Commission expects to **sign up to 1** framework partnership. The action plan shall foresee a **progressive increase** (from a 10% baseline) of tasks to be subcontracted to **eligible cross border** SME/Midcaps or to eligible entities which are not dependant from the consortium

members and their affiliated entities. The share allocated to these ‘newcomers’ will be taken into account in the award criteria.

The Commission reserves the right not to award any SGA under the FPA, depending on the available budget, the existence of co-financing for development activities, or the quality of the proposals received and the results of the evaluation.

Eligibility

For the framework partnership, the eligibility of entities check will be done generally at FPA-level for all applicants and then again only in advance of amendment of the FPA (e.g., change of a partner, change of ownership/status requiring a new assessment).

Duration

The framework partnership agreement will have a duration of four years. The budgetary amount envisioned for the duration of the Framework Partnership Agreement is EUR 100 000 000. Applicants must **provide a high-level 4-year multiannual action plan and budget** for the period 2023-2026. The duration of activities proposed under the multiannual action plan may exceed the duration of the FPA but corresponding SGAs must be signed before the end of the FPA.

Project budget

Specific grants’ budgets are expected to range indicatively between EUR 10 000 000 and EUR 40 000 000.

Financial and operational capacity and exclusion

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.

For framework partnerships, the financial capacity check will be done only once at FPA-level for all applicants.

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).

For framework partnerships, the operational capacity check will be done generally at FPA-level and then again for each grant application in the calls for specific grants.

For framework partnerships, exclusion will be checked before FPA signature and then again before signature of each specific grant).

Evaluation and award procedure

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

No commitment for funding — Invitation to FPA preparation does NOT constitute a commitment for funding.

Grant preparation will involve a dialogue in order to fine-tune technical or financial aspects of the project and may require extra information from the applicants. 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 framework partnership.

2.6. EDF-2022-LS-RA-SMERO

- **Targeted type of actions:** Research actions (dedicated to SMEs and research organisations).
- **Form of funding:** Lump sum grants following the call for proposals
- **Targeted type of applicants:** Any eligible consortium as defined in Articles 9 and 10(4) of the EDF Regulation. Members of the consortium need to be SMEs (as defined in Commission Recommendation 2003/361/EC) or research organisations. The coordinator of the consortium needs to be an SME. The budget allocated to research organisations cannot exceed 40% of the total requested grant amount.
- **Indicative budget for the call:** The Union is considering a contribution of up to EUR 17 600 000 to support one call topic:

2.6.1. EDF-2022-LS-RA-SMERO-NT: Non-thematic research actions by SMEs and research organisations

- **Number of actions to be funded:** Several actions, addressing different solutions, may be funded for this topic
- **Range of financial contribution of the Union per proposal:** The requested funding should not exceed EUR 4 000 000.

Objectives

This call encourages the driving role of innovative SMEs in bringing forward innovation defence research, possibly by adapting technologies from civil applications or addressing hybrid warfare.

Successful SME beneficiaries may be offered Business Coaching, to reduce the time of bringing the results to the next phase, e.g., development.

Scope and types of activities

Scope

The proposals must address innovative technologies and solutions for defence, including those that can improve readiness, deployability, reliability, safety and sustainability of forces in defence tasks and missions, for example in terms of operations, equipment, infrastructure, energy solutions, surveillance systems or digital solutions.

The proposals can address any subject of interest for defence.

Types of activities

The following types of activities are eligible for this topic:

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)	Yes
(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
(c)	Studies , such as feasibility studies to explore the feasibility of new or upgraded products, technologies, processes, services and solutions	Yes
(d)	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, including partial tests for risk reduction in an industrial or representative environment	Yes
(e)	System prototyping of a defence product, tangible or intangible component or technology	No
(f)	Testing of a defence product, tangible or intangible component or technology	No
(g)	Qualification of a defence product, tangible or intangible component or technology	No
(h)	Certification of a defence product, tangible or intangible component or technology	No
(i)	Development of technologies or assets increasing efficiency across the life cycle of defence products and technologies	No

However, the proposals must not cover studies only.

The proposals must describe a clear work breakdown structure and link the proposed tasks to eligible activities.

Proposals should include clear descriptions of the proposed criteria to assess work package completion.

Functional requirements

This call is open to any technological research for defence. Proposals should describe the targeted functionalities and the foreseen means to measure progress toward the achievements of these functionalities.

Expected impact

- Innovative and cost-effective solutions for defence applications.

- Ground-breaking or novel concepts and approaches, new promising future technological improvements or the application of technologies or concepts previously not applied in the defence sector.
- Enhanced innovation capacity across Europe by involvement of SMEs that can make a difference in the future.
- Potential for future market creation for SMEs, especially by facilitating access of SMEs to defence markets and supply chains.
- Contribution to the development of European research and technology ecosystems and to the strengthening of European defence supply chains.

2.7. EDF-2022-LS-DA-SME

- **Targeted type of actions:** Development actions (dedicated to SMEs).
- **Form of funding:** Lump sum grants following the call for proposals
- **Targeted type of applicants:** Any eligible consortium as defined in Articles 9 and 10(4) of the EDF Regulation. Members of the consortium need to be SMEs (as defined in Commission Recommendation 2003/361/EC)
- **Indicative budget for the call:** The Union is considering a contribution of up to EUR 36 500 000 to support one call topic:

2.7.1. EDF-2022-LS-DA-SME-NT: Non-thematic development actions by SMEs

- **Number of actions to be funded:** Several actions, addressing different solutions, may be funded for this topic
- **Range of financial contribution of the Union per proposal:** The requested funding should not exceed EUR 4 000 000.

Objectives

This call encourages the driving role of innovative SMEs to turn technology and research results into defence products in a fast and cost-efficient way, possibly by adapting technologies from civil applications or addressing hybrid warfare.

Successful SME beneficiaries may be offered Business Coaching, to reduce the time of bringing the results to the next phase of development.

Scope and types of activities

Scope

The proposals must address innovative defence products, solutions and technologies, including those that can improve readiness, deployability, reliability, safety and sustainability of forces in defence tasks and missions, for example in terms of operations, equipment, infrastructure, energy solutions, surveillance systems or digital solutions.

The proposals can address any subject of interest for defence.

Types of activities

The following types of activities are eligible for this topic:

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
(c)	Studies , such as feasibility studies to explore the feasibility of new or upgraded products, technologies, processes, services and solutions	Yes
(d)	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, including partial tests for risk reduction in an industrial or representative environment	Yes
(e)	System prototyping of a defence product, tangible or intangible component or technology	Yes
(f)	Testing of a defence product, tangible or intangible component or technology	Yes
(g)	Qualification of a defence product, tangible or intangible component or technology	Yes
(h)	Certification of a defence product, tangible or intangible component or technology	Yes
(i)	Development of technologies or assets increasing efficiency across the life cycle of defence products and technologies	Yes

However, the proposals must address at least one activity among design, system prototyping, testing, qualification, certification and increasing efficiency.

The proposals must describe a clear work breakdown structure and link the proposed tasks to eligible activities.

Proposals should include clear descriptions of the proposed criteria to assess work package completion.

Functional requirements

This call is open to any technology development for defence. Proposals should describe the targeted functionalities and the foreseen means to measure progress toward the achievements of these functionalities.

Expected impact

- Innovative, rapid and cost-effective solutions for defence applications.
- Ground-breaking or novel concepts and approaches, new promising future technological improvements or the application of technologies or concepts previously not applied in the defence sector.
- Enhanced innovation capacity across Europe by involvement of SMEs that can make a difference in the future.
- Potential for future market creation for SMEs, especially by facilitating access of SMEs to defence markets and supply chains.
- Contribution to the development of European technological and industrial ecosystems and to the strengthening of European defence supply chains.

2.8. EDF-2022-CSA-NFP

- **Management mode:** Action managed by the Commission in direct management
- **Form of funding:** Grant following the call for proposals
- **Indicative budget for the call:**
The Union is considering a contribution of up to EUR 1 500 000
- **Applicable maximum funding rate:**
100% of the eligible costs of the action (Article 186(2)(a) of the Financial Regulation), notwithstanding the co-financing principle in accordance with Article 190(1) of the Financial Regulation).

The maximum Union financial contribution will be calculated based on the total eligible costs (direct and indirect) provided and justified by the applicants at the time of submission of the proposal (see Annex 2 to the Submission form).

Indirect eligible costs must be determined by applying a flat rate of 25% of the total direct eligible costs of the action, excluding costs of subcontracting, support to third parties and any unit costs or lump sums which include indirect costs.
- **Number of actions to be funded:** Up to one action may be funded
- **Duration of the action:** The recommended duration of the action is 3 years.

The National Focal Points for the EDF (EDF-NFPs) consists of a network of individuals nominated by Member States and countries associated to the European Defence Fund (EDF) that are supported by national structures established under the responsibility and control of the Member States and Associated Countries. The NFPs form an essential part of the EDF implementation by providing practical information, advice, training, and other forms of assistance to stakeholders on all aspects of participation in the EDF.

Objectives

The objectives of this call are:

- To enhance the functioning of the EDF-NFP network and contribute to the increase of the impact of the EDF in maximising the competitiveness of EU defence industry, its capacity to innovate and contribute to developing key technologies for the future;
- To strengthen cross-border collaboration between EDF-NFPs and to improve coordination in EDF-NFP-related activities that reach more than one Member State or Associated Country;
- To continuously improve the services of the individual EDF-NFPs with respect to all aspects of participation in the EDF and to all stakeholders concerned;
- To foster matchmaking activities to facilitate the forming of consortia participating in the EDF calls
- To enhance the cooperation of EDF-NFPs with the Enterprise Europe Network and other relevant networks

Scope

This action aims at facilitating trans-national cooperation between EDF-NFPs with a view to identifying and sharing good practices and raising the general standard of support to (potential) programme applicants, taking into account the diversity of actors that could benefit from the programme and thus contribute to strengthening the European defence industry.

The action should cover:

- NFP-organised joint trainings to improve the services they provide, share experiences and best practices in relation to their support for the EDF;
- Twinning arrangements/facilities (in person visits or virtual), where NFPs can learn from their counterparts about the different approaches adopted in supporting national entities' participation in the EDF;
- The development of information and promotional materials (both in digital and physical formats) that can be used by the whole NFP network, relating to the services the NFP network is providing and on practical aspects of participating in the EDF;
- The organisation of cross-border matchmaking events at selected international and European defence fairs or at national information activities such as national EDF info days;
- The setting up of a website providing information about the services supported by the action, including, but not limited to listing relevant events, introducing the EDF with a special focus on entities that are new to defence research and development, and a facility to conduct partner search taking into account existing platforms and practices;
- The development of methodologies to help EDF-NFPs to interact with Enterprise Europe Network that has already well-established contacts with entities that are active in civilian R&D and can facilitate matchmaking;
- Interaction with relevant national industry associations and with relevant Horizon Europe NCP networks, with the objective to have a wider reach to industrial entities and make the EDF better known.

Special attention should be given to enhancing the competence of EDF-NFPs, including helping less experienced EDF-NFPs rapidly acquire the know-how built up in other countries.

The action should provide clearly defined and quantified deliverables and milestones in line with the activities mentioned in the scope of this topic.

NFPs that choose not to participate as a member of the consortium, are nevertheless invited and encouraged to participate in the action activities (e.g., workshops), and the costs incurred by the consortium for such participation (e.g., travel costs paid by the consortium) may be included in the estimated budget and be eligible for funding by the Commission.

Expected impact

- Increased awareness about and visibility of opportunities provided by the EDF, as well as stronger participation of newcomers to the programme, incl. SMEs in particular;
- Enhanced NFP services across the Union and Associated Countries in the defence area, providing solid support to (potential) programme applicants;
- Consistent level of support given to their respective stakeholders by NFPs across the European Union and Associated Countries.

Eligibility conditions

Applicants must be the national support structures hosting EDF-NFP or alternate EDF-NFP officially nominated to the Commission by a Member State or an Associated Country. A consortium should consist of national support structures of at least 10 Member States or Associated Countries.

Subcontractors involved in the action, including their management structure and their infrastructure, facilities, assets and resources which are used for the purposes of the action to be supported by the Fund, must be established in:

- the Member States of the European Union (EU), including their outermost regions, and the overseas countries and territories (OCTs) linked to them;
- the members of the European Free Trade Association which are members of the European Economic Area (EEA), in accordance with the conditions laid down in the Agreement on the EEA (associated countries), unless these members have opted out of the EDF.

For the purposes of the action supported by the Fund, subcontractors involved in the action must not be subject to control by a non-associated third country or by a non-associated third-country entity.

In the event of a change during the carrying out of the action which might put into question the fulfilment of the eligibility criteria, the relevant legal entity must inform the Commission, which will assess whether those eligibility criteria continue to be met and will address the potential impact of that change on the funding of the action.

Selection criteria

Financial capacity

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

Are exempted from financial capacity check:

- public bodies (entities established as a public body under national law, including local, regional or national authorities) or international organisations; and
- applicants requesting grant amounts less than EUR 60 000 (low-value grant).

Operational capacity

Applicants must have the know-how, qualifications and resources to successfully implement their tasks in the action and contribute their share (including, where appropriate, sufficient experience in EU/transnational projects of comparable size).

Exclusion

Applicants that are subject to EU administrative sanctions (i.e., exclusion)⁵⁵ or are in one of the exclusion situations⁵⁶ that bar them from receiving EU grants can NOT participate.

Award criteria

Excellence

- Clarity and pertinence of the action's objectives and corresponding targets.
- Quality of the proposed measures, including soundness of methodology.

Impact

- Credibility of the pathways to achieve the expected outcomes and impacts specified in the call for proposals, and the likely scale and significance of the contributions from the action.
- Suitability and quality of the measures to maximise expected outcomes and impacts, as set out in the dissemination and exploitation plan, including communication activities.
- Extent to which the beneficiaries of the consortium have a reach in all EU Member States and associated countries, by involving a maximum number of NFPs in the consortium directly and openness of activities to non-beneficiary NFPs.

Quality and efficiency of the implementation

- Quality and effectiveness of the work plan, assessment of risks, and appropriateness of the effort assigned to work packages, and the resources overall.
- Capacity and role of each participant, and the extent to which the consortium as a whole brings together the necessary expertise.

Evaluation scores will be awarded for the criteria. For applications, each criterion will be scored out of 5. The threshold for individual criteria will be 3. The overall threshold, applying to the sum of the three individual scores, will be 10.

Proposals that pass the individual threshold and the overall threshold will be considered for funding, within the limits of the available call budget. Other proposals will be rejected.

⁵⁵ See Article 136 EU Financial Regulation 2018/1046.

⁵⁶ See Articles 136 and 141 EU Financial Regulation 2018/1046.

Proposals will be checked for formal requirements (admissibility and eligibility) and then evaluated by an evaluation committee for operational capacity and award criteria and then ranked according to their quality score.