European Defence Industrial Development Programme (EDIDP)

2020 calls for proposals, conditions for the calls and annexe

based on
Regulation (EU) 2018/1092
and on
Commission implementing Decision C(2019) 2205

Version 1.2
23 July 2020

HISTORY OF CHANGES			
Version	**Publication Date**	**Change**	**Page**
1.0	19 March 2020	Initial version	
1.1	19 May 2020	Hour of deadline for submission changed to correspond to the one on the Portal.	102-103
		Flexibility clause regarding date of provision of common requirements/common technical specifications.	108
1.2	23 July 2020	In the topic EDIDP-UCCRS-MUAS-2020: - in the section "Targeted activities", replacement of the reference to "robotized mine warfare systems" by "underwater warfare systems"; - in the section "Main high-level requirements", addition of missing footnotes for MAD and LIDAR.	23
		In the topic EDIDP-CUAS-2020: - in the section "Scope", addition of the missing footnote; - in the section targeted activities, removal of the reference to "qualification" and "certification" since they are not required (although possible as part of downstream activities).	30 31
		In the topics EDIDP-NGPSC-LRIF-2020 and EDIDP-NGPSC-PGA-2020, in the section "targeted activities" removal of useless reference to "upstream activities".	69, 71
		Participation of UK: precision that "subcontractors" refer to "subcontractors involved in the action".	110
		Typos and layout issues.	1, 4-5, 7-8, 11, 16, 35, 40, 78-79, 82-83, 116-118, 120-122, 124-125, footnotes

Table of contents

1. Introduction

1.1. Implementation of the European Defence Industrial Development Programme (EDIDP)

The EDIDP is an industrial development programme, established by Regulation (EU) 2018/1092[1] (hereafter EDIDP Regulation), which is implemented through annual calls for proposals in 2019 and 2020. The calls are based on a two-year work programme defined in close cooperation with Member States and adopted by the Commission on 19 March 2019.

1.2. Scope and content of the document

This document contains the 2020 EDIDP calls for proposals, the conditions for the calls and an annexe. It includes budgetary information, the criteria which the Commission will use to evaluate the proposals as well as other important information for applicants.

In line with the work programme, there will be twelve calls for proposals in 2020, among which nine calls addressing the three priority areas defined in the EDIDP Regulation:

1. Preparation, protection, deployment and sustainability (three calls);
2. Information management and superiority and command, control, communication, computers, intelligence, surveillance and reconnaissance (C4ISR), cyber defence and cyber security (three calls);
3. Engagement and effectors (three calls).

and three calls addressing cross-domain capabilities, among which one is specifically dedicated to Small and Medium-sized Enterprises (SME) as mentioned in the EDIDP Regulation in order to encourage the participation of such enterprises and foster innovation:

The 2020 calls related to *Preparation, protection, deployment and sustainability* are addressing the following categories:

- Chemical Biological Radiological Nuclear (CBRN) detection capabilities and medical countermeasures (call EDIDP-CBRN-2020);
- Underwater control contributing to resilience at sea (call EDIDP-UCCRS-2020);
- Counter Unmanned Air Systems (UASs) capabilities (call EDIDP-CUAS-2020).

The 2020 calls related to *Information management and superiority and command, control, communication, computers, intelligence, surveillance and reconnaissance (C4ISR), cyber defence and cyber security* are addressing the following categories:

[1] Regulation (EU) 2018/1092 of the European Parliament and of the Council of 18 July 2018 establishing the European Defence Industrial Development Programme aiming at supporting the competitiveness and innovation capacity of the Union's defence industry, OJ L 200 of 7.8.2018, p. 30.

- Cyber situational awareness and defence capabilities, defence networks and technologies for secure communication and information sharing (call EDIDP-CSAMN-2020);
- Space Situational Awareness (SSA) and early warning capabilities (call EDIDP-SSAEW-2020);
- Maritime surveillance capabilities (call EDIDP-MSC-2020).

The 2020 calls related to *Engagement and effectors* are addressing the following categories:

- Upgrade of current and development of next generation ground-based precision strike capabilities (call EDIDP-NGPSC-2020);
- Ground combat capabilities (call EDIDP-GCC-2020);
- Air combat capabilities (call EDIDP-ACC-2020).

The 2020 call related to *Cross-domain capabilities* is addressing the following category:

- Simulation and virtualisation tools and equipment for training, exercises, systems design, development and integration, testing and validation (call EDIDP-SVTE-2020);
- Defence technologies supported by artificial intelligence (call EDIDP-AI-2020);
- Innovative and future-oriented defence solutions (call EDIDP-SME-2020).

Some of the above-mentioned categories and related calls cover several topics of interest.

Important information

The detailed content of these calls is described in section 2 of this document.
The conditions related to these calls are provided in section 3 of this document and in the annexe to this document.

Finally, it is reminded that a call for expression of interest to establish a list of experts to assist the Commission with tasks in connection with EDIDP is published on the Commission's website[2]. The Commission will select experts from this list to perform assessments of the proposals submitted by the applicants in response to the calls described hereafter in this document.

1.3. Key website

All information relating to the present calls for proposals can be accessed from the Commission's "Funding and tenders portal" website:
https://ec.europa.eu/info/funding-tenders/opportunities/portal/screen/programmes/edidp

[2] https://ec.europa.eu/growth/content/call-expression-interest-establish-list-experts-assist-european-commission-tasks-connection_en.

1.4. Reference documents

1.4.1. Basic texts

[Financial Regulation] - Regulation (EU, Euratom) 2018/1046 of the European Parliament and of the Council of 18 July 2018 on the financial rules applicable to the general budget of the Union, amending Regulations (EU) No 1296/2013, (EU) No 1301/2013, (EU) No 1303/2013, (EU) No 1304/2013, (EU) No 1309/2013, (EU) No 1316/2013, (EU) No 223/2014, (EU) No 283/2014, and Decision No 541/2014/EU and repealing Regulation (EU, Euratom) No 966/2012[3].

[EDIDP Regulation] - Regulation (EU) 2018/1092 of the European Parliament and of the Council of 18 July 2018 establishing the European Defence Industrial Development Programme aiming at supporting the competitiveness and innovation capacity of the Union's defence industry.

[EDIDP Work Programme] - Commission implementing Decision (C)2019 2205 on the financing of the European Defence Industrial Development Programme and the adoption of the work programme for the years 2019 and 2020.

1.4.2. Documents needed to apply

This document and its annexe.
The submission form and its annexes (available here).

1.4.3. Additional documents

Guide for applicants (available here after the opening of the calls).
The model grant agreement and its annexes (available here after the opening of the calls).

[3] OJ L 193, 30.7.2018, p. 1–222.

2. Calls

The EDIDP calls for proposals for 2020 are described in this section.

2.1. Call EDIDP-CBRN-2020 – Chemical Biological Radiological Nuclear (CBRN) detection capabilities and medical countermeasures

The resilience of the Union and its preparedness to deal with CBRN threats needs to be enhanced, and there are significant cooperation opportunities on CBRN reconnaissance, decontamination, individual and collective protection, as well as on training. A comprehensive set of CBRN capabilities must be capable of providing CBRN scientific and operational assessment and advice to commanders and their staffs during the planning and conduct of operations.

The 2018 Capability Development Plan (CDP) indicates the relevance of deploying dedicated Intelligence, Surveillance, Target Acquisition and Reconnaissance (ISTAR), exploitation and processing capabilities and specialised sensors for detection and early warning of potential CBRN threats to friendly populations and defence forces. Early detection of CBRN threats can be supported by intelligence operations performed through web data mining in dark nets and deep web.

Proposals are invited against any of the following topics

- **EDIDP-CBRN-DEWS-2020:** Capabilities for CBRN risk assessment, detection, early warning and surveillance;
- **EDIDP-CBRN-MCM-2020:** CBRN medical countermeasures, such as preventive and therapeutic immunotherapy.

Budget

The Union is considering a contribution of up to EUR 13 500 000 to support proposals addressing any of the above-mentioned topics and their associated specific challenge, scope, targeted activities and main high-level requirements.

Several actions, addressing different topics, may be funded under this call.

1.1.1. Topic EDIDP-CBRN-DEWS-2020 – Capabilities for CBRN risk assessment, detection, early warning and surveillance

CBRN threat is increasing worldwide with proliferating states, terrorists' organizations and even "lone wolves" desiring not to limit their actions to conventional means.

This topic addresses the need for a CBRN surveillance capability limiting the risk for soldiers by using remotely operated platforms and providing commanders and when needed, civilian authorities, with a consolidated CBRN picture.

CBRN surveillance is the capability to observe and collect, including via sampling, information on CBRN threat indicators along with an ability to detect, identify and monitor CBRN substances and Environmental and Industrial Hazard (EIH) contamination. This collected information feeds into the CBRN information management system and forms the basis for timely, accurate and relevant CBRN advice.

Specific challenge

The specific challenges of the topic reside in:

- the need for a simple, easy-to-use, remotely-operated solution for CBRN detection, monitoring and sampling in hazardous environments;
- setting up the basics for a European-built CBRN reconnaissance architecture.

Scope

The proposals must address the development of a whole CBRN reconnaissance and surveillance system, based on unmanned ground and aerial vehicles for CBR detection, monitoring and sampling, to be used by a CBRN surveillance team (embarked or disembarked).

Targeted activities

The proposals must cover the design, system prototyping and testing of a whole system in a representative environment with simulants and live agents, not excluding upstream or downstream activities.

Main high-level requirements

The proposed system should fulfil the following requirements:

1. General

- The system should consist in a set of different and inter-related tools:
  - a mission planning tool;
  - a mission execution tool composed of:
    - an unmanned aerial system (UAS);
    - an unmanned ground system (UGS);
    - a CBRN SaaS[4] data fusion cell;
    - a CBRN SaaS control element.
  - a set of CBRN sensor payloads (sensors);

[4] Software as a service.

  - a set of CBRN sampling payloads (samplers).
- The system should be deployed and operated by a CBRN surveillance team, embarked or disembarked;
- The system should be able to interface with CBRN Command and Control (C2) and relevant information systems, directly or indirectly;
- The system should be useable during day and night and under high temperature (A2) and low temperature (C2) weather conditions and austere conditions (as defined in AECTP[5]-230).

2. <u>“Mission-planning” and “mission execution” tools</u>

- The mission-planning tool should allow operators, while assisting them, to:
  - select the payloads to be carried by both UAV and UGV;
  - define (where necessary) the pathways to be followed by the unmanned platforms;
  - establish the detection strategy;
  - establish the sampling strategy;
  - establish the decontamination strategy, where necessary.
- The mission execution tool should:
  - allow the operators to control and pilot the unmanned platforms;
  - allow the operator to operate sensors and samplers in real time;
  - provide a real time video feedback of the unmanned platforms cameras;
  - provide real-time feedback on sensors and samplers installed onto the unmanned platforms: status, alarms, concentrations detected, identification or classification if possible and any other relevant information for the mission;
  - record and store the missions;
  - be able to replay the missions.
- All user interfaces (UI) should:
  - be consistent;
  - be user friendly;
  - reduce cognitive load;
  - keep users in control and always provide them with essential information available.
- The “mission-planning” and “mission execution” tools should:
  - convert all data into a CBRN operational picture for the military/civil leader in accordance with NATO STANAGs ATP-45 and AEP-45;
  - provide an interface for the fusion of the CBRN operational picture with the common operational picture (preferable in accordance with NATO STANAG 5525 (MIP standard));
  - provide an interface to export all suitable data from sensor and calculated data into formatted messages in accordance with NATO STANAG 7149 (APP-11);
  - provide an interface to export UAS, UGS and CBRN SaaS control element location and status data in accordance with NATO STANAG 5527 (ADatP-36), Friendly Force Tracking Systems (FFTS) interoperability.

3. <u>UAS and UGS</u>

- The systems should incorporate a set of unmanned platforms with the following characteristics:

[5] Allied environmental conditions and test publication.

  - platforms should consist in at least:
    - a UGV for ground R&C detection and RBC sampling;
    - a rotary wing UAV and a fixed wing UAV for aerial R&C detection and RBC sampling.
  - platforms should be COTS[6] (only applies to the prototype) and modified only to adapt sensors and samplers payloads according to the mission;
  - platforms should be equipped with day and night and IR (at least thermal) cameras;
  - platforms should be sized in order to transport at least both detection and sampling payloads for a dedicated mission (C, B or R);
  - UAV platforms should be sized to transport the complete set of payloads for C&R detection and CBR sampling;
  - UAV platforms should be operable in VLOS (visual line of sight) and BLOS (beyond line of sight);
  - UGV platform(s) should be sized to transport the complete set of payloads for C&R detection and CBR sampling;
  - platforms should be able to provide their own geolocation data (position) for real time display in the mission execution tool;
  - platforms should have sufficient energy autonomy for the intended reconnaissance mission including time to reach the mission site and back:
    - mission ranging from 30 min to 180 min for UAV;
    - distance to mission site: at least 2 000 m for UAV and at least 1 500 m for UGV.
  - platforms should include a 3D topographic reconnaissance tool and a second aerial rotary wings platform dedicated to high-resolution video-monitoring of the mission site.
- The UGS should:
  - be able to mark the contaminated area according to NATO ATP-3.8.1 Vol I;
  - be able to collect the samples from UGV, easy to handle by individuals wearing IPE7 in accordance with STANAG 4701 (AEP66);
  - have a level 1 protection, according to NATO STANAG 4569;
  - use hybrid (diesel and battery) wheeled or tracked vehicle;
  - be able to operate in rough terrain;
  - be able to operate in an area with very high radiation of at least 4 Gy/h.
- The UAS should:
  - be field deployable at any point in the mission area;
  - be able to return to designated point after loss of communication with the operator;
  - be able to take airborne environmental samples (for both rotary and fixed wing vehicles);
  - be able to land with the rotary wing system in the contaminated area to detect and identify liquid chemical substances and take full spectrum of environmental samples (plant material, solids, water, other liquids);
  - be able to transmit all data in real time to the CBRN SaaS control element.

4. <u>CBRN data fusion cell</u>

- The CBRN data fusion cell should be:

[6] Commercial off-the-shelf.

[7] Individual protective equipment.

  - able to convert all data into a CBRN operational picture for the military/civil leader in accordance with NATO STANAGs 2103 (ATP-45) and STANAG 2497 (AEP-45);
  - able to provide an interface for the fusion of the CBRN operational picture with the common operational picture (preferable in accordance with NATO STANAG 5525 (MIP standard));
  - able to provide an interface to export all suitable data from sensors and calculated data into formatted messages in accordance with NATO STANAG 7149 (APP-11);
  - able to provide an interface to import suitable data beyond the scope of CBRN SaaS formatted in accordance with NATO STANAG 7149 (APP-11) and/or STANAG 2103 (ATP-45).

5. CBRN control element

- The CBRN control element should be able to:
  - transport the UGS and the UAS including accessories (*i.e.* all necessary equipment needed for the operation of the platforms);
  - remotely control (wireless) the UAS and UGS;
  - provide local weather data during operations;
  - provide its own location data (position);
  - ensure the reception, local storage and extraction (net ready) of sensor data from the UAS/ UGS;
  - alert or warn the operators in case received sensor data show the presence of CBRN threats/hazards;
  - transmit raw sensor data including images and real time videos to the CBRN SaaS data fusion cell;
  - control the platforms in accordance with NATO STANAG 4586 (AEP-84).

6. Sensors

- Sensors should be packaged in payloads. Smaller UAVs (< 25 kg) should have sensors packed in modular payloads;
- Modular sensors' payloads for smaller UAVs (< 25 kg) should be seamlessly plugged in the platform and in the mission execution tool and send their data in real-time;
- C sensors should be able to:
  - detect, provide class identification and measured concentration of a list of CWAs[8], to be defined with the participating Member States;
  - detect, identify and provide measured concentration of a list of TICs[9], to be defined with the participating Member States;
  - to maintain detection performance, according to specifications in military relevant environments, in the presence of commonly encountered interfering chemicals to be defined with the participating Member States.
- R sensors should be capable of detecting and identifying radiological materials (X-rays, gamma-rays sources), and of determining the extent of the radiological contamination;
- Sensor payloads should integrate passive or active aerosols and/or gas stand-off detection.

[8] Chemical warfare agents.

[9] Toxic industrial chemicals.

7. Samplers

- The system should be able to collect and take back samples for further analysis;
- Samplers should be packaged in modular payloads;
- Modular samplers' payloads should be seamlessly plugged in the platform and in the mission-execution tool;
- Samplers should be able to collect representative (both qualitatively and quantitatively) samples of CBR agents;
- Samplers should be able to collect:
  - aerosols (UAV, UGV);
  - liquids (UGV mandatory, UAV if possible);
  - gas/vapours (UAV, UGV);
  - swabs (UGV).
- Samples should be stored in order not to represent a secondary contamination source when the platforms are back.

Expected impact

- To provide EU military forces with a mission-customizable, cost-effective solution for CBRN threats early detection, identification, risk assessment and surveillance;
- To provide EU military forces with consistent CBRN detection, sampling and monitoring against a large panel of threats;
- To set up a European-built CBRN reconnaissance architecture.

2.1.2. Topic EDIDP-CBRN-MCM-2020 – CBRN medical countermeasures, such as preventive and therapeutic immunotherapy

The objective of this topic is to develop medical counter-measures (MedCM) for EU military forces to face current and emerging CBRN threats (mainly of biological and chemical nature). It thus aims at developing common and shared capabilities for EU military against chemical/biological crisis generated by a natural or provoked event and at treating pathologies or injuries of significant impact. It will thus contribute to respond more efficiently to external conflicts and crises.

Specific challenge

Such medical counter-measures are currently poorly studied by both academia and industry within the EU due to:

- their specificity;
- the large funding to be engaged for R&D;
- the low occurrence of such threats even though they are proliferating worldwide (thus increasing operational risks for military forces);
- current EU regulations on medicines.

Scope

The proposals must address the development of medical counter-measures (MedCMs) against the chemical, bacteriological and radiological threats listed in the main high-level requirements below.

Targeted activities

The proposals must cover the design, prototyping and testing of one or several MedCMs, not excluding upstream or downstream activities.

Compared with the development of a standard medicine these activities must be understood as:

- design: preclinical, *in vitro* studies;
- prototyping: preclinical, *in vivo* studies[10];
- testing: clinical, phase I studies[11].

The targeted activities must in particular include:

- the evaluation of state-of-the-art research in order to identify best MedCM candidates;
- the definition of preclinical studies to be performed to develop the best therapeutic or prophylactic candidates;
- the realisation of preclinical studies;
- the realisation of phase I clinical studies;
- the building of relevant documentation for marketing authorization based on the former activities.

[10] The data or information on the kinetics and pharmacodynamics of the product or other relevant data or information, in animals and primates, will allow selection of an effective dose in humans.

[11] Phase II and III clinical studies are considered as “qualification” and marketing authorisation is considered as “certification”.

Main high-level requirements

The proposed MedCMs should fulfil the following requirements:

1. General

- Efficacy of the MedCMs should be demonstrated on relevant animal models as close as possible as humans during preclinical studies, according to the recommendations of national or European regulatory agencies;
- Innocuity should be demonstrated on human volunteers during phase I clinical trials;
- The final product is to be administered by medical personnel, at medical treatment facilities.

2. Chemical threat

- To develop an efficient MedCM against severe poisoning by any nerve agent or organophosphorus pesticide with, for example, a stoichiometric bioscavenger isolated from human plasma such as human butyrylcholinesterase (BuChE) enzyme from the IV-4 Cohn plasma fraction.

3. Biological threat

- To develop an efficient MedCM against toxins poisoning or any B agent for which classical treatments (*e.g.* antibiotics) are not available with for example immunotherapy.

4. Radiological threat

- To develop an efficient radionuclides chelator to treat internal or external radiological contamination of personnel.

Expected impact

- Provide EU military forces with consistent CBRN medical protections against a large panel of threats;
- Facilitate the development of CBRN defence capabilities that each Member State or individual government or industry cannot face solely;
- Develop EU autonomous industrial segments.

1.2. Call EDIDP-UCCRS-2020 – Underwater control contributing to resilience at sea

Considering the increasing defence maritime forces in the world and the importance of the freedom of manoeuver at sea, naval interdiction and force protection are key preconditions to be met before any deployment and power projection from sea. The 2018 Capability Development Plan (CDP) identifies the need for an improved ability to detect, identify and neutralise or avoid/deceive subsurface threats, including active and passive measures. The 2018 CDP highlights the importance of mine warfare, anti-submarine warfare and harbour protection.

Proposals are invited against any of the following topics

- **EDIDP-UCCRS-MCM-2020:** Solutions to detect, identify, counter and protect against mine threats (including those operating at very high depths);
- **EDIDP-UCCRS-MUAS-2020:** Solutions to detect, identify, counter and protect against mobile manned, unmanned or autonomous underwater systems (including those operating at very high depths);
- **EDIDP-UCCRS-EDD-2020:** Enhanced defence diving solutions to detect, identify, counter and protect against sub-surface threats.

Budget

The Union is considering a contribution of up to EUR 22 500 000 to support proposals addressing any of the above-mentioned topics and their associated specific challenge, scope, targeted activities and main high-level requirements.

Several actions, addressing different topics, may be funded under this call.

1.2.1. Topic EDIDP-UCCRS-MCM-2020 – Solutions to detect, identify, counter and protect against mine threats (including those operating at very high depths).

Mine-countermeasures capability is an increasing concern worldwide (including for several EU Member States), in particular the necessity to come up with disruptive and robust solutions in order to tackle the ever-evolving hostile environment taking advantage of technological progress.

Both technical know-how and operational expertise are required to come up with performing, competitive solutions able to face up with the worldwide competition.

It is a topic where the European Union can take benefit of the already-existing ecosystem and expertise within its Member States in order to reinforce its strategic position.

Specific challenge

Among the future challenges that mine-countermeasures solutions will have to tackle there will be:

- **at mission management level**: the ability for operator(s) to handle and process increasingly complex, multi-source data;
- **at mission level**: the necessity to optimize conditions of handling unmanned systems for safe operations and mission time optimization;
- **at unmanned system level**: the ability to operate in more and more complex conditions (deeper, GPS denied…) and to process data inside unmanned systems in order to increase their autonomy.

Scope

The proposals must address the development of next-generation mine-countermeasures solutions.

These solutions must include both manned and unmanned systems, Command, Control, Communication, Computers and Information (C4I) and mission management systems, sensors, as well as manned-unmanned teaming, and their basing, launching and retrieval, to detect, identify, counter and protect against mine threats (including those operating at very high depths).

Targeted activities

The proposals must cover at least the design or the prototyping of the solutions, not excluding upstream and downstream activities such as feasibility study and testing in an operational environment.

The targeted activities must in particular include:

- the collection and analysis of end-user’s requirements;
- the definition of operational priorities;
- the definition of performance indicators to evaluate technical solutions versus the end-user’s requirements;
- the design or system prototyping;

- simulations to create realistic scenarios allowing to work on new operational concepts of use for robotized mine warfare systems and to optimize the sizing and design of the solutions;
- the elaboration of roadmap(s) for further developments.

<u>Main high-level requirements</u>

The proposed solutions should fulfil the following requirements:

1. <u>General</u>

- Should improve and speed up detection, classification and identification of mines or mine-like objects, especially in most demanding conditions (deep water, turbidity, floating or sub surface, buried…), using innovative sensors and/or UUVs[12] and embedded computing;
- Should have improved capabilities for neutralization of innovative mines such as deep self-propelled mines and mine counter-counter measures anticipation (dummy mines);
- Should have improved capabilities for easy maintenance and management of unmanned systems energy/data on board mothership and/or USVs[13] or underwater (*e.g.* underwater docking stations);
- Should have a globally improved mission management system via innovative manned-unmanned man-to-machine interfaces and increased decision autonomy (*e.g.* use of artificial intelligence);
- Should have improved acoustic stealthiness (*e.g.* use of embedded dynamic anti-vibration solutions);
- Should implement "cybersecurity by design" principles to develop a system resilient to cyber-attacks (which could lead to data flow disruption and information leakages);
- Should be consistent with relevant NATO standards.

The proposed solutions can be based on a modular concept of manned and unmanned systems.

2. <u>Demining operations</u>

- Should aim at keeping human out of danger zone (*e.g.* demining operations are performed by remotely controlled or autonomous unmanned systems);
- The manned assets possibly needed for the working of the system should provide mine protection for personnel and equipment by providing vessels with low signatures, good manoeuvrability and high shock resistance;
- Should remain efficient in GNSS degraded or denied environments including long range navigation;
- Should aim at finding and neutralizing all kinds of mines including the most innovative ones in harsh environments such as great depths, sea states 4 plus, current 3 kts plus;
- Should become more and more autonomous with human tasks limited to supervision and control. The neutralization of mines should remain with a human in the loop (HITL).

[12] Unmanned underwater vehicles.

[13] Unmanned surface vehicles.

3. Global improvement of the mission management system

- Development of innovative Man to Machine Interface (MMI) taking into account future Mine Counter Measures (MCM) challenges hence addressing operator management missions (simultaneous roll out of autonomous vehicles air/surface/underwater; planning);
- Development of decision-making support layer at mission management system level (system functioning assessment; data assessment; de-confliction; water space management; prevention of mutual interference);
- Development of decision-making support layer applicable for unmanned vehicle level (heterogeneous data, extraction/fusion/classification/identification from various sensors) enabling enhanced autonomy and improved security;
- Improvement of interoperability between European systems, either at sea or for exchanges of post-mission data (sharing of data and improvement of software…).

4. Docking solution

- Design of a (fix or mobile) docking station enabling data transmission, energy recharging and maintenance operations.

Expected impact

- Identify and confirm the key technological breakthroughs enabling to tackle future challenges of counter mining activities;
- Enable globally an enhanced performance of MCM activities;
- Support the development of a competitive and efficient ecosystem able to position a true, consolidated European offer in MCM domain;
- Improve interoperability of European mine countermeasures systems and make the work in coalition easier, including the formation and training of operators.

1.2.2. Topic EDIDP-UCCRS-MUAS-2020 – Solutions to detect, identify, counter and protect against mobile manned, unmanned or autonomous underwater systems (including those operating at very high depths).

Specific challenges

Among the future challenges that underwater warfare solutions will have to tackle there will be:

- **at mission management level**: the ability for operator(s) to handle and process increasingly complex, multi-source data;
- **at mission level**: the necessity to optimize conditions of handling assets such as unmanned systems or sensors for safe operations and mission time optimization;
- **at systems level**: the necessity to optimize at early stage detection, identification, classification and neutralization of underwater manned, unmanned and autonomous systems that are floating, sailing or bottoming subsurface. Different architectures of systems could be proposed with sensors, mission systems management and inter-connections between the different sub-systems of the architecture proposed. These could include usual assets generally employed for these tasks like Maritime Patrol Aircrafts (MPA) with appropriate sensors or could include more innovative solutions including UAV[14] or other assets;
- **at unmanned system level**: ability to operate in more and more complex conditions (deeper, GPS denied…) and to process data inside the unmanned system in order to increase its autonomy.

Scope

The proposals must address the development of next-generation underwater warfare solutions.

These solutions must include both manned and unmanned systems, Command, Control, Communication, Computers and Information (C4I) and mission management systems, sensors, as well as manned-unmanned teaming, and their basing, launching and retrieval, to detect, identify, counter and protect against mobile manned, unmanned or autonomous underwater systems (including those operating at very high depths).

Targeted activities

The proposals must cover at least the design or the prototyping of the solutions, not excluding upstream and downstream activities such as feasibility study and testing in an operational environment.

The targeted activities must in particular include:

- the collection and analysis of end-user's requirements;
- the definition of operational priorities;
- the definition of performance indicators to evaluate technical solutions versus the end-user's requirements;
- the design or system prototyping;

[14] Unmanned air vehicle.

- simulations to create realistic scenarios allowing to work on new operational concepts of use for underwater warfare systems and to optimize the sizing and design of the solutions;
- the elaboration of roadmap(s) for further developments.

Main high-level requirements

The proposed solutions should fulfil the following requirements:

1. General

- Should improve and speed up detection, classification and identification of objects especially in most demanding conditions (deep water, turbidity, floating or sub surface…) using, for example, innovative sensors, new methods for machine/deep learning, artificial intelligence and/or UAVs/UUVs and embedded/low energy computing;
- Should include improved or new generation of sensors (radar, MAD[15], active and passive sonobuoys, optical devices, LIDAR[16]…) including those embedded on MPAs or UxVs;
- The combat system architecture should be designed so as to decrease the workload of crews, to enable operations with unmanned systems of all kind and to improve the connectivity and the interoperability with the naval forces;
- Should have improved capabilities for neutralization of innovative underwater threats such as unmanned systems, divers, torpedoes, manned systems (including submarines);
- Should have improved capabilities for underwater data (including video and audio) communication with control platform and between unmanned systems;
- Should have improved capabilities for advanced sea floor mapping;
- Should have improved capabilities for easy maintenance and management of unmanned systems energy/data on board control platform and/or USVs or underwater (*e.g.* underwater docking stations);
- Should have a globally improved mission management system via innovative manned-unmanned man-to-machine interfaces, data visualisation and increased decision autonomy (*e.g.* use of artificial intelligence);
- Should have an integrated management platform;
- Should have improved stealthiness (*e.g.* use of embedded dynamic anti-vibration solutions);
- Should implement “cybersecurity by design” principles to develop a system resilient to cyber-attacks (which could lead to data flow disruption and information leakages);
- Should be consistent with relevant NATO standards.

The proposed solutions can be based on a modular concept of manned and unmanned systems.

2. Underwater warfare operations

- Should aim at keeping human out of danger zone (*e.g.* operations are performed by remotely controlled or autonomous unmanned systems);

[15] Magnetic anomaly detector.

[16] Light detection and ranging.

- Should remain efficient in GNSS degraded or denied environments including long range navigation;
- Should aim at finding and neutralizing all kinds of underwater threats including the most innovative ones in harsh environments such as great depths, sea states 4 plus, current 3 kts plus;
- Should become more and more autonomous with human tasks limited to supervision and control. The neutralization of threats should remain with a human in the loop (HITL).

3. Global improvement of the mission management system

- Development of innovative Man to Machine Interface (MMI) and data visualisation capabilities, taking into account future underwater mobile threats challenges hence addressing operator management missions (simultaneous roll out of autonomous vehicles air/surface/underwater; planning);
- Development of decision-making support layer, for example based on advanced data analytics and precise predictions, at mission management system level (system functioning assessment; data assessment; de-confliction; water space management; prevention of mutual interference);
- Development of decision-making support layer applicable for unmanned vehicle level (heterogeneous data, extraction/fusion/classification/identification from various sensors) enabling enhanced autonomy and improved security.

4. Docking solution

- Design of a (fix or mobile) docking station enabling data transmission, energy recharging and maintenance operations.

5. New generation of sensors for air assets and architecture

- Improvement of sensors for air assets (UAV or MPA) and architecture should take into account the need for improved performance against quiet submarines or small objects like UUVs. On the other hand, the capability to operate in a discrete way *vis-à-vis* the threat is of utmost importance and the way to use the sensors or to use the unmanned systems should be studied accordingly.

Expected impact

- Identify and confirm the key technological breakthroughs enabling to tackle future challenges of countering underwater mobile threats;
- Enable globally an enhanced performance of underwater warfare activities;
- Support the development of a competitive and efficient ecosystem able to position a true, consolidated European offer in underwater warfare domain;
- Allow the detection of the submarine threats by modern sensors, with no limitations imposed by a non-European country;
- Prepare the combat system of the next generation of MPAs, with a high level of connectivity to naval assets and unmanned systems.

1.2.3. Topic EDIDP-UCCRS-EDD-2020 – Enhanced defence diving solutions to detect, identify, counter and protect against sub-surface threats.

Diving capabilities are a strategic asset, where critical gaps are currently identified within the EU. Enhanced defence diving is needed to support the full spectrum of underwater intervention operations in expeditionary setting, both at sea and in inland bodies of water. The developed diving related capabilities should respond to 2018 CDP priorities with regard to manoeuvre at sea, protection of sea lines of communications and underwater regulated zones, enhancement of the resilience of EU critical maritime infrastructure and the conduct of mine counter measures (MCM).

Specific challenges

Diving activities in general involve a risk which is a sum of many diving specific and nonspecific factors (risk components), some of which are not fully studied yet and are to be addressed by tailor-made and innovative solutions based on cutting-edge and disruptive technologies.

- **Ability to avoid/mitigate Decompression Sickness (DCS) risk.** Although scientists have focused on studying the decompression process for a long time, the basic principles are not fully understood yet. The current decompression models are mostly empirical and hypothetical and do not fully reflect the actual behaviour and reactions of the human body during decompression. DCS risk is influenced by individual human susceptibility and by intra-individual changes in susceptibility on a day-by-day basis. There is also a gap for innovative technologies for reliable and effective medical support and recovery of divers, such as technologies tailored to individual real-time diving profiles, which increases the efficiency of DCS avoidance/mitigation and provides flexibility and efficiency in case of decompression accident.
- **Ability to create and use a real-time underwater common operational picture** through the fusion of various types of information, as a collaborative planning and task-execution tool at all levels, thus enhancing operational effectiveness through a unified information exchange system.
- **Necessity to ensure interoperability, coordination and de-confliction of underwater intervention activities, including manned-unmanned teaming**, involving employment of a big number of divers and UUVs simultaneously (swarm). The methods and systems in use are often obsolete, imprecise or not reliable enough for defence application.

Scope

The proposals must address the development of next-generation comprehensive solutions for enhanced defence diving to detect, identify, counter and protect against sub-surface threats.

These solutions must include medical support system for physiological support and recovery of divers in case of decompression sickness problem, C4I mission systems for underwater management, underwater monitoring, situational awareness, positioning, navigation and manned-unmanned teaming. The proposed solutions must in particular cover the following areas:

- decompression sickness (DCS) risk mitigation;

- underwater positioning, tracking, wireless communications and data transfer subsurface and subsurface-surface over great distance;
- manned-unmanned teaming in swarm mode setting (underwater AIS).

Targeted activities

The proposals must cover at least the design or the prototyping of the solutions, not excluding upstream and downstream activities such as feasibility study and testing in an operational environment.

The targeted activities must in particular include:

- the collection and analysis of end-user's requirements;
- the definition of operational priorities;
- the definition of performance indicators to evaluate technical solutions versus the end-user's requirements;
- the design or system prototyping, including simulation;
- the elaboration of roadmap(s) for further developments.

Main high-level requirements

The proposed solutions should fulfil the following requirements:

- the system should support lower tactical level operations in underwater environment and should comply with applicable military and/or civil standards. It should in particular be consistent with relevant NATO standards;
- the tactical comprehensive modular information and support system should demonstrate low electromagnetic footprint and should be modular, providing scalability according to the operational needs;
- the system should support suitable interoperability standards for exchange of C2[17] data and ISR[18] products to be ready for integration into an overall information management infrastructure in order to enable net-centric operations;
- the system should incorporate a navigation subsystem capable of operation in a GNSS degraded or denied environment;
- the system should support extended autonomy mode operations without external power source;
- the system should have swarming capabilities in underwater manned-unmanned settings;
- the system should be easily deployable and recoverable;
- cybersecurity by design principles should be followed to develop a system resilient to cyber-attacks, which could lead to data flow disruption and information leakages;
- adoption of open architecture design principles with regards to the subsystems so as to facilitate the incorporation of new components and platforms and advances in standards and protocols, especially those related to interoperability.

The proposed solutions should include:

- a component for real time monitoring, registering and data transmission of relevant physiological parameters of diver(s) underwater;

[17] Command and control.

[18] Intelligence, surveillance and reconnaissance.

- a component for real time automatic calculation of individualized diving decompression profile, taking into account the following variables as a minimum: individual body characteristics; current physiological parameters of the diver; the diving equipment being used and the chosen breathing gas. The calculated/optimized decompression profile should be visualized in real time, both for the diver underwater and for the diving supervisor on the surface;
- a component for divers' support and recovery based on the real time profiles of the divers;
- a component providing a solution to operate in case of decompression sickness problem, employing transportable and easy deployable hyperbaric unit;
- a component for tracking and visualization (on the surface) of the real time location of diver(s) working underwater;
- a component for data transmission and information flow between surface and underwater and in underwater environment;
- Man to Machine Interface (MMI) between manned and unmanned systems ensuring interoperability, coordination and de-confliction of underwater activities, including manned-unmanned teaming in swarm mode setting, when multiple divers and UUVs (AUVs[19], ROVs[20], *etc.*) are being employed simultaneously.

The proposed solutions can be based on a modular concept of comprehensive systems, providing information, monitoring, communications, positioning, support management and situational awareness and manned-unmanned systems teaming.

Expected impact

At strategic level:

- to identify and confirm the key technological breakthroughs enabling to tackle future challenges in defence diving domain;
- to enable globally an enhanced performance of underwater activities related to defence diving;
- to support the development of a competitive and efficient ecosystem able to position a true, consolidated European offer in defence diving domain.

At mission level:

- to decrease the reaction time and improve the situational awareness of EU forces during tactical operations in underwater environment, effectively contributing to the generation of near real time COP[21] development, particularly with regards to own forces and assets tracking (underwater/diving AIS[22]), and diving and UUV operations information products dissemination;
- to facilitate the integration of the tactical comprehensive modular information system outputs with other sources from Member States, EU forces, NATO and civil agencies through the reinforcement of information exchange interoperability;
- to maximize the capability of the tactical comprehensive modular information system to operate efficiently by incorporation of technological advances in underwater and radio

[19] Autonomous underwater vehicles.

[20] Remotely operated vehicles.

[21] Common operational picture.

[22] Automatic identification system.

communications, navigation and autonomy (including manned-unmanned teaming and swarming) as well as its ease of use;

- to provide early warning for potential underwater diving accidents by real time information and visualization of relevant current physiological parameters of divers and their exact location underwater, enabling timely automated identification of possible hazardous health conditions and expeditious help in case of need, including via unmanned system(s).

1.3. Call EDIDP-CUAS-2020 – Counter Unmanned Air Systems (UASs) capabilities

Due to the growing threat of a wide range of UAVs[23] (including consumer mini-drones increasingly used for defence purposes), the need to develop active and passive countermeasures against armed and intelligence gathering UASs has been identified to increase force protection, critical infrastructure resilience, and information security. Emphasis needs to be placed on defence products with an inherent modularity, scalability and interoperability in design including Command and Control (C2) and decision support capabilities in order to cover applications ranging from protection of individual soldier, vehicle and command post to protection of larger critical infrastructure, including in urban areas.

Proposals are invited against the following topic

EDIDP-CUAS-2020: Capabilities to detect, classify, track, identify and/or counter UASs in defence scenarios.

Budget

The Union is considering a contribution of up to EUR 13 500 000 to support proposals addressing the above-mentioned topic and its associated specific challenge, scope, targeted activities and main high-level requirements.

Several actions may be funded under this call.

Specific challenges

Small UAVs, including cheap Commercial off the Shelf (COTS) and easy to assemble UAS components, are widely available and their popularity is even growing.

Traditional surveillance systems fail to cope with these objects because of their characteristics. Indeed their low speed make them invisible to conventional radars, their low altitude allows them to hide amongst trees or behind buildings, their very small RF[24], thermal and acoustic signatures makes them difficult to detect. Additionally the high manoeuvrability of some machines makes their movement hard to track once detected, and their increasing on-board processing capabilities (*e.g.* automated and vision based navigation, use of Artificial Intelligence) makes them more resilient to “First Generation” C-UAS systems that rely on RF detection and jamming.

Scope

The proposals must address the development of a counter UAS capability covering detection, tracking, classification, identification, risk assessment and neutralisation of the UAS threat, taking into account task assignment and coordination.

[23] Unmanned Aerial Vehicles. While UAV refers to the aircraft only (*e.g.* unmanned platform), a UAS includes one or more UAVs, a ground control system and the communication link.

[24] Radio frequency.

The proposals must focus on the classes of UAVs as described in the following table (class II is optional):

TAXONOMY (coherent with NATO)		**Reference information regarding UAV threats**			
Threat	**Weight [kg]**	**Reference size [cm^3]**	**Max speed [km/h]**	**Typical altitude [m]**	**Typical RCS[25] [dBm^2]**
Class I (a) and (b) - micro	< 2 kg	25 x 25 x 30	80	100	-20 (objective -30)[26]
Class I (c) - mini	> 2 & < 20	40 x 40 x 30	100	1 000	-13 (objective -20)
Class I (d) - small	> 20 & < 150	200 x 150 x 50	150	1 500	-10
Class II - tactical	> 150 & < 600	1 000 x 700 x 100	300	3 000	-3

The proposals must take into account the following considerations:

Threats to safety and security

- Safety concerns due to the potential for recreational drones to enter unauthorized areas either by accident or negligence.
- Security concerns caused by malevolent users attempting deliberately hostile missions such as the delivery of IEDs, smuggling or ISR.

Operational environment

Threats must be considered in their environmental and operational context. Mitigation options vary from civilian and military scenarios and between urban and rural settings. Solutions will differ according to the size of the area to protect, the reaction time required and the need to minimize fratricide and collateral damage. Missiles or air-burst munitions are unacceptable in a civilian context and may not be the best solution in urban peacetime environments. A soft kill approach may be required to safely take over drones carrying a suspected IED in a crowded place, notwithstanding the potential for electro-magnetic fratricide and collateral damage and notwithstanding current inability to determine the intent of an unexpected drone intrusion. However, many current soft kill solutions are likely to be ineffective against a fully autonomous UAS. Accordingly, a suite of solutions will be required to comply with a broad set of rules of engagement (RoEs) each adapted to the surrounding environment and the operational scenario (including the transition from peace-time to war-time).

Deployment

C-UAS systems must cover both fixed and deployed applications.

- **Fixed applications**: Forward Operating Bases (FOBs) and critical infrastructures may demand continuous operation, day & night 24/7, at reasonable operational and maintenance cost.

[25] Radar Cross Section.

[26] As "objective" it is meant a key technical specification which, being really challenging, must be striven during the industrial development but which does not constitute a constraint for the final achievement of the capability required.

- **Deployed, "pop-up" applications**: Tactical military activities as well as civil events demand quick deployment with minimum logistic support, and the rapid integration of additional sensors and effectors within a recognised open architecture.

Multi-UAV Systems

Threats can occur by mean of either single or multiple UAV units, either uncoordinated or operating as a team or as a single system (swarm). Therefore, C-UAS systems must be scalable to adapt to the level of expected threat and must offer the proper reaction.

Targeted activities

The proposals must cover one or more of the following activities: study, design, prototyping or testing of the proposed solution, not excluding downstream activities.

These activities must in particular cover one or more of the following:

- feasibility studies, capability gaps analysis, CONOPS definition, system specification, preliminary requirements review (PRR) and architecture definition;
- studies about promising technologies that nowadays have a technology readiness too low to successfully integrate and deploy in the field;
- detailed design of the system, including the System Requirements Review (SRR), the Preliminary Design Review (PDR) and Critical Design Review (CDR);
- Prototyping;
- Testing in relevant operational scenarios.

Main high-level requirements

The drivers for the C-UAS capability design should be:

- open, flexible, modular and scalable architecture based on a plug-and-play component approach which allows deployment of specific configurations adapted to the threat scenarios;
- robustness and high availability;
- standard interfaces and interoperability;
- day and night operational capability;
- fast deployability;
- minimum logistic support;
- cost-effectiveness and relevance of neutralisation solutions to the characteristics of the threat and to the operational environment;
- configurability of the solution for the different operational environments enabling end-users to complement/adapt as required the architecture (with more mobile/deployable components for example), to choose sensors, effectors, active areas and create tailor-made instances of the system, completely adapted to their specific needs.

The system should ensure effectiveness in the following operational scenarios:

- protection of Forward Operating Bases (FOB);
- protection of critical areas (with tailored approaches and deployment in case of point objective, "extended point" objectives and area objectives), including urban environment;
- protection of strategic assets;

- protection of moving assets (*e.g.* convoys, fleets, *etc.*).

The C-UAS systems should address all operational phases:

- planning:
  - mission planning;
  - report function.
- deployment:
  - full operational set-up.
- mission conduct:
  - generating real time operational picture;
  - automated and real time warning;
  - modern and ergonomic graphical interface;
  - threat tracking;
  - optimal selection and activation of effectors;
  - threat neutralization with focus on semi-autonomous (or even manual) technical solutions (HITL[27]).

The system should fulfil the following requirements:

- detect, classify, track, identify and counter UASs (single and/or multi-UAVs) in defence scenarios using multiple technologies; the ability of the proposed solution from detection to counter UASs also in civil scenarios is considered a significant plus;
- deliver and update real-time operational picture and alerts;
- integrate into multilayer C2 system with cross-security-domain approach;
- provide a range of selective mitigation alternatives with the ability to evaluate mission success probabilities and resulting drawback;
- require limited logistic support for deployment and maintenance;
- require minimum operator effort for decision making;
- provide dynamic scalability of sensors and effectors;
- facilitate the incorporation of counter UASs in security and defence systems for fixed and deployed asset;
- able to operate in a wide range of climate (*e.g.* arctic, subtropical) and weather (*e.g.* rain, fog, snow) conditions.

All the active and passive sensors and the effectors should be integrated and connected in a local command and control station. This station should implement data fusion and automatic procedures and rules in order to focus human operations on action, resources coordination and cooperation.

The proposed system should in particular include the following capabilities:

- Detection, recognition, classification, identification and assessment: for these purposes the autonomous processing of information should be balanced across the adopted sensors and timely reported to the central C2 to reduce operational manpower load and bottlenecks. Solutions based on omnidirectional detection (rotating or staring) while also

[27] Human in the loop.

capable of limiting the detection to a sector of choice will be preferred for its higher flexibility of adoption;

- Sensors and effectors should use communication protocols that allow "plug-and-play" deployment and should be able to operate without impacting on existing communications or position / navigation Infrastructures;
- Command and control: C2 should plan and monitor subsystems' missions and conditions, merge information from heterogeneous sensors, report about any internal or external elements that could affect the system performances, evaluate the possible engagement approaches to the operator, coordinate the engagement approach selected by the operator and report on the resulting outcomes. C2, as part of threat evaluation and weapon assignment, should compute success probability, time to complete the neutralization and drawback probabilities for each of the possible neutralization approaches. In addition, C2 should allow subsystems' dynamic deployment and multi-instance integration. In order to allow smart and effective deployment, C2 and related subsystems should be at the lowest possible security classification level while at the same time be able to interoperate with other C2 systems (*e.g.* air defence systems) at higher security classification level;
- Neutralization: neutralisation should include effectors compatible with the operational environment and the characteristics of the threat (including multiple UAVs elimination). These may for example include navigation systems spoofing, RF jamming, kinetic effectors (soft/hard with lethal or non-lethal effects), catch or hit-to-kill by a swarm subset or direct energy weapons (*e.g.* high power lasers and/or microwaves).

Expected impact

- Stimulate the production of doctrine and CONOPS in this field;
- Develop a comprehensive C-UAS capability;
- Reduce the minimum reaction time;
- Enhance situation awareness and protection of critical areas and strategic assets;
- Ensure interoperability with existing security and defence systems.

1.4. Call EDIDP-CSAMN-2020 – Cyber situational awareness and defence capabilities, defence networks and technologies for secure communication and information sharing

The 2018 Capability Development Plan (CDP) points to an increasing risk of communication networks disruption through cyber-attacks. It also underlines that cyber technologies, such as cyber situational awareness technologies and defensive cyber technologies are essential to counter cyber security threats faced by Member States, and in particular, the Union and Member States' command and control structures from tactical to strategic level.

It also identifies the need to communicate and share information through employing deployable interoperable communications systems and data-sharing platforms (including data storage and sharing capabilities), *ad-hoc* and distributed networks.

Proposals are invited against any of the following topics

- **EDIDP-CSAMN-SDN-2020:** Software defined network for defence use including the development of products and technologies;
- **EDIDP-CSAMN-EDICT-2020:** Easily deployable and interconnected cyber toolbox for defence use.

Budget

The Union is considering a contribution of up to EUR 14 300 000 to support proposals addressing any of the above-mentioned topics and their associated specific challenge, scope, targeted activities and main high-level requirements.

Several actions, addressing different topics, may be funded under this call.

1.4.1. Topic EDIDP-CSAMN-SDN-2020 – Software defined network for defence use including the development of products and technologies

Specific challenge

The main benefits of adopting network architectures based on the Software Defined Network (SDN) paradigm in defence networks at strategical, infrastructural and technology levels are known:

- agility and flexibility;
- ‘independency’ on the network elements’ technology;
- capability to efficiently use network resources;
- broader situation awareness;
- faster responses to events;
- *etc.*

Through the decoupling of network control and forwarding functions, SDN lets network control become programmable, and the underlying infrastructure be abstracted from applications and network services. SDN makes networks more flexible and easier to manage, simplifying and automating labour-intensive network management functions, service development and deployment, easier to re-configure and to interoperate among diverse networks.

Nevertheless, challenges for SDN remain when considering tactical networking, especially when carrying out *ad hoc* communications and information sharing. Tactical edge/deployable networking is probably the most challenging area where SDN can be used, but at the same time the one that can benefit the most from this new technology.

For strategical and infrastructural domains, SDN network architectures are typically centralized architectures that rely on a single SDN controller communicating with the SDN switches and the applications. Such architectural approach does not have to be automatically replicated for tactical networks which specific characteristics can be quite demanding: bandwidth constraints, links’ instability, frequent network topology changes, limited devices’ capabilities (battery and storage capacity, CPU[28] power), high dynamicity (frequent mission reconfigurations and high mobility of nodes), stringent Quality of Service (QoS) requirements, presence of legacy networking elements, the need for redundancy and resilience for communications and information sharing and against cyber-attacks.

These characteristics, together with the increasing need for day zero interoperability within coalition federated scenario, require that SDN technologies and solutions for tactical applications are selected on a case-by-case basis.

One of the challenges is to identify the proper SDN technologies and solutions that allow to select the SDN network architecture which is the most suitable for the tactical edge/deployable network that has to be established on the basis of:

- the operational requirements of the mission;

[28] Central processing unit.

- the available resources (*e.g.:* mobile elements on the field, available transmission means, heterogeneity of the network elements);
- the environmental/electromagnetic conditions and cyber threats of the operational scenario.

This challenge includes the capability to have SDN enabled products that allow to carry out the proper SDN architecture, with a high level of centralization or a distributed architecture such as a full SDN or hybrid (mix of pure SDN technology and legacy technology) network architecture, wherever and whenever it is needed.

Scope

The proposals must address the development of SDN solutions (including the development of technologies and products), for a network architectural framework which provides EU armed forces with the needed information to select the most proper network architecture. This network architecture must be suitable for the operational scenario and mission requirements referring to specific operational use cases, based on CONOPS coming from the end users (armed forces).

This capability is to be shown in tactical edge/deployable applications by looking at the benefits for voice communications and C2 services and highlighting, where applicable, how the interactions with intelligent software defined radio device (*e.g.* cognitive radio), SDN enabled, can further improve the effectiveness of the mission.

The SDN architecture must be as much as possible suitable to support the new emerging defence technology against cyber-attacks in order to be effective not only for the network situational awareness, but also for the cyber situational awareness.

Targeted activities

The proposals must cover the study, design, prototyping and testing of the proposed SDN solution, not excluding downstream activities.

The targeted activities must in particular include:

- the definition of the set of reference operational use cases on the basis of the CONOPS and requirements of the end users that have to be envisaged in the network architecture framework;
- a feasibility implementation study of the applicability of the selected SDN technologies to existing/future products, in a coalition SDN federated scenario. This study must be undertaken as guideline to be taken into consideration for the definition of the interoperability standards in tactical coalition networks (*e.g.* to be taken into consideration within the Federated Mission Networking initiative);
- the development of the network architecture framework which allows to identify the most suitable SDN network architecture for the reference operational use cases;
- the development of SDN controllers and switches functions that can be hosted on the same devices so as to make the same equipment suitable to be used in a centralized or distributed SDN network according to the operational needs, or to be used as backup SDN node in case of redundant architecture;

- the identification of the Software Defined Radio (SDR) device and suitable waveforms characteristics enabling for SDN usage;
- the development of the proper northbound and southbound API[29] to allow to see the benefits for voice and C2 services;
- the development of the functions to be used for communications among different SDN controllers in distributed architecture and exploring applications in federated scenarios;
- field experiments and system validation.

Main high-level requirements

The proposed SDN solutions should allow:

- a centralized SDN network architecture;
- a distributed SDN architecture with a hierarchical/redundant structure;
- the consideration of hybrid SDN/legacy architecture, highlighting the benefits for mission critical applications in emergency situations;
- the use of SDN-enabled SDR device, when equipped with the proper waveforms (*e.g.* including cognitive functions), at least as SDN switches/data planes.

The proposed SDN technologies and solutions should fulfil the following requirements:

- the developed SDN solutions should address ground deployable platforms and mobile vehicles/dismounted soldiers;
- the SDN solutions should be optimized for the intended use, taking into account the available computing power, the volume and weight constraints and the available power supplies;
- the selected SDN technologies and the development of SDN based/enabled products should be able to form a centralized SDN architecture or a distributed architecture;
- the SDN architecture should guarantee redundancy and resilience against network elements failures and network link loss, such as quick capability to adapt to network topology updates due to insertion of new network elements;
- the SDN solutions and network architecture should consider the presence in the tactical network of UAV and UGV as network elements providing information relevant at C2 level for situational awareness and, in the future, for cyber situational awareness;
- the SDN network elements should be capable to interoperate with the proper SDR device supporting the proper waveform;
- the SDN solutions and network architectures should guarantee an efficient use of network resource and spectrum;
- the adopted SDN network architecture should be used to carry out voice and C2 services with respect to their QoS[30] requirements.

Expected impact

- Enhance agility, scalability and network management flexibility for tactical edge/deployable network;
- Simplify policy deployment for network management, quality of service, routing, cyber defence;

[29] Application programming interface.
[30] Quality of service.

- Optimize the use of network resources and spectrum and rely on routing and networking traffic management strategies aiming at guaranteeing that the stringent Quality of Service requirements for the services are met on ‘per flow/service’ basis;
- Increase the resilience of tactical networks, speed up reactions to network topologies changes due to instability, end user operational mission requirements, high mobility of the network nodes;
- Enable cognitive networking via the interaction with SDN enabled SDR devices;
- Provide network architecture solutions suitable and adoptable in tactical coalition operation by the armed forces of the involved EU Member States;
- Leveraging the SDN benefits to tactical edge networking including the unmanned air and ground vehicles network segments;
- Allow the sustainable evolution of the European military missions exploiting the possibility to host legacy capabilities on modern technologies, without requiring to update or change the whole network but only properly acting on the applications and their interfaces with the SDN networking elements;
- Improve situational awareness and leverage on the agility enhanced by SDN solutions to defend or prevent cyber-attacks in order to enhance the security of EU tactical operations.

1.4.2. Topic EDIDP-CSAMN-EDICT-2020 – Easily deployable and interconnected cyber toolbox for defence use

Specific challenge

The main challenge is to create a new generation of mobile cyber toolbox to be used by cyber rapid response teams (CRRTs) to manage cyber incidents (detect, investigate and remedy hostile activities) in defence field, as well as government environment and critical information infrastructure.

Usually, CRRTs are deployed as mobile teams to deal with cyber incidents on its premises or from remote locations, possibly with limited access to secure communication means. In the modern environment, the dependency also for military operations from civilian infrastructure (including industrial systems) and civilian solutions is growing rapidly with emerging technologies such as 5G and IoT (Internet of Things).

Although there are many rapid response initiatives and many rapid response teams formed both in civilian and military organizations, they have limitations. These teams are usually able to operate only in common enterprise environments (*e.g.* Microsoft and Linux based environments), have limited capabilities for specialized systems, or are dedicated to work only in organizations' internal networks. Therefore, these teams lack skills and tools to operate in multi-site and multi-organization environments. On the other hand, they are restricted to work in their own networks by legal constraints and technological means.

Currently, a number of home-grown and relatively well-established tools and training – both commercial and open source- are available. Large companies active in cybersecurity have also built cyber toolboxes for internal and external use.

These toolsets are, however, best suited to relatively conventional scenarios and may not be convenient to use or highly effective in transnational military and government environments.

Some of the limitations include:

- the packaging and architecture of such solutions, the integration with back-office investigation capabilities and the ability to face narrow network bandwidth;
- the stealthiness of the deployed tools on potentially compromised networks;
- the ability to face other, non-traditional types of systems, such as industrial control systems and SCADA[31].

Scope

The proposals must address the development of capabilities for CRRTs to manage effectively cyber incidents in the various above-mentioned environments and fields.

These capabilities (hardware and software) must be integrated smoothly and comprehensively in an easily deployable (including via commercial airlines) cyber toolbox.

The toolbox must address the following areas:

Data collection, reporting, and reach back

- Stealthy data collection tools on potentially affected systems;
- Ticketing system;

[31] Supervisory control and data acquisition.

- Communication platform;
- Big data exchange platform;
- IoC[32] sharing platform.

Monitoring, log aggregation

- Firewalls, IDS[33]/IPS[34], including required network interface adapters, duplicators, taps, *etc.*;
- Data collections tools and SIEM[35];
- Operating systems scanning, including deep and proven boot sanity checks of various Windows, Mac OS and Linux distributions, including in the virtualized environment;
- Firmware scanning (USB, Ethernet, and Wi-Fi-based).

Analysis and forensics capability

- Analysis of the deployable tool output, including the analysis of acquired images and network traffic;
- Fast, configurable data lake for logs and network activity analysis;
- Connection with cyber threat intelligence.

ICS/SCADA capability

- Tools required for data collection and analysis in industrial environments, addressing the most common ICS/SCADA elements' manufacturers, protocols, interfaces, *etc.*;

Vulnerability assessments and penetration testing capability

- Tools (hardware and software) for vulnerability assessment and penetration testing.

Targeted activities

The proposals must cover the study, design, prototyping and testing of the cyber toolbox, not excluding downstream activities.

The targeted activities must in particular include:

- the review of the typical current capability of a CRRT, the activities such team performs, and the types of automated support that such a team needs. This must consider, among other things:
    - the possible functional gaps in current toolsets;
    - the impact of virtualized/cloud type environments on tool deployment and scalability;
    - the extent to which integration of different tools might simplify operator tasks and improve the effectiveness of a deployment;
    - the definition of a process to manage the evolution of the tools among many participating entities.

[32] Indicator of compromise.
[33] Intrusion detection system.
[34] Intrusion prevention system.
[35] Security information and event management.

- the review of the implications of operating in widely distributed and interoperable environments, in particular, considering how CRRTs operate in constrained environments such as the military deployed environment;
- the review of the advanced team operating models that enable collaborative distributed activity, critically necessary to contain or manage large scale attacks enabling mission assurance, taking into account the questions of need-to-know/need-to-share and communications with command and control systems;
- based on these analyses, identification of specific enhancements that must be made to current generation toolsets, processes and practices;
- the design, prototyping and testing of a new generation toolset implementing these enhancements;
- exercises to inform operating processes and practices across the full operating domain;
- collective exercises (*i.e.* across multiple sites/systems/teams) to further develop operating processes and practices.

Main high-level requirements

The toolbox should consist of four principal parts:

1) **Workplace**. Laptops with the appropriate software;
2) **Sensors**. Deployable network sensors, including data collection interfaces;
3) **Back-office infrastructure**. Back-office infrastructure and services;
4) **Cloud**. Cloud services, SaaS tools, commercial data feeds.

1. Workplace
   - The workplace should consist of a set of identically prepared laptops, provided together with additional accessories, like external hard drives, taps, duplicators, interfaces, cables, adaptors, also specific forensic tools (such as Tableau hardware);
   - Laptops should contain all required software for identified CRRT tasks, including, but not limited to, incident handling, monitoring, forensics, vulnerability assessment, penetration testing, back-office communication;
   - Software for monitoring, log collection, and analysis of ICS[36]/SCADA environments, covering at least the 20 most popular ICS/SCADA protocols should be provided;
   - A virtualization environment should be installed for running virtual machines. If specific applications need Linux or other OS, they should be prepared inside appropriate virtual machines.

2. Sensors
   - Deployable sensors should be provided for collecting network traffic;
   - A sensor should be composed of one or more servers, routers, switches, duplicators, taps, adapters, interfaces, and other hardware accessories for connecting to various networks and infrastructures;
   - Everything should be fitted into an easily transportable, ruggedized box/frame. The box weight and dimensions should allow it to be transportable by commercial airlines;
   - The toolbox should contain two identical sensors (for redundancy, training, and testing).

[36] Industrial control system.

3. Back-office infrastructure
    - The back-office infrastructure consists of one or more servers and data storage to be installed in a central (home) location. It is meant to provide required services for the CRRT:
        - IoC[37] sharing platform (*e.g.* MISP[38]);
        - Ticketing system (*e.g.* RTIR[39]);
        - Communication platform (*e.g.* MatterMost);
        - Big data exchange platform (*e.g.* NextCloud);
        - Collaboration platform (*e.g.* GitLab, Confluence);
        - Git repository (*e.g.* GitLab).
    - Infrastructure should support the ability to install other required tools and services.

4. Cloud
    - Cloud should be understood as a set of cloud services and commercial SaaS tools.
    - This should at a minimum include:
        - commercial data feeds;
        - commercial signatures for sensors;
        - threat intelligence platform.

Other common requirements for the toolbox

- Modular structure. Components should be able to work independently and to be removed or replaced;
- The toolbox should be based on open standards and common best practices to facilitate interoperability with existing national cybersecurity systems, including, but not limited to, cyber situation awareness, cyber threat intelligence, and command and control platforms. This means using common open import/export formats, existing interfaces, and the use of APIs throughout individual tools;
- Deployable tools on a potentially compromised network and systems should be stealthy and auditable;
- Analysis of collected data should be able to be done both manually and automatically;
- The proposed solution should consist of necessary hardware and software for online and offline investigation;
- The toolbox should be able to provide the analysts with an autonomous capability (analyse the collected data on a deployable system), while being able to interconnect with back-office in different network availability conditions, to get threat intelligence, send analysis results, *etc.*;
- The proposed solution should provide dynamic, scalable, and resilient solutions, capable of easily integrating all the actors and nodes involved in each mission;
- The proposed solution should allow rapid installation (for example – on new servers or new laptops), restoring/reverting, administration and operation;
- Toolbox (workplaces, sensors) should be easily deployable overseas, including via commercial airlines;

[37] Indicators of compromise.

[38] Malware information sharing platform.

[39] Request tracker for incident response.

- The proposed solution should include training materials sized for not less than 120 hours of appropriate training;
- Delivery of the project – a fully functioning, ready to use toolbox.

Expected impact

- Developing new generation tools and procedures for defensive cyber operations in any operational context;
- Improving readiness and response capability for unconventional cyber-attacks in the Member States;
- Improve cyber incident prevention, mitigation, investigation and reporting capabilities in the Member States for large scale cyber-attacks impacting both civilian as well as military environment;
- Support the development of Member State's cyber defence capabilities and decision-making in cyber emergencies.

1.5. Call EDIDP-SSAEW-2020 – Space Situational Awareness (SSA) and early warning capabilities

The 2018 Capability Development Plan (CDP) points to a shortfall in the SSA and space surveillance domain. It highlights the need for highly accurate, real-time space situational awareness through collation, analysis and exploitation of information collected by space-based and terrestrial sensors. A relevant set of SSA capabilities must allow to nullify or reduce the effectiveness of hostile actions in order to ensure access to and use of space enabled capabilities.

Proposals are invited against any of the following topics

- **EDIDP-SSAEW-SC2-2020:** Advanced Space Command and Control (SC2) capability to process and exploit SSA data generated from sensors and catalogues to provide a complete space picture;
- **EDIDP-SSAEW-SSAS-2020:** Enhanced SSA sensors for accurate identification and characterization of existing Geostationary Earth Orbit (GEO) and Low Earth Orbit (LEO) public and private assets;
- **EDIDP-SSAEW-EW-2020:** Early warning against ballistic missile threats through initial detection and tracking of ballistic missiles before handing over to ground based radars.

Budget

The Union is considering a contribution of up to EUR 22 500 000 to support proposals addressing any of the above-mentioned topics and their associated specific challenge, scope, targeted activities and main high-level requirements.

Several actions, addressing different topics, may be funded under this call.

The Commission will pay particular attention to the civil and dual-use on-going initiatives at Union level to avoid unnecessary duplication.

1.5.1. Topic EDIDP-SSAEW-SC2-2020 – Advanced Space Command and Control (SC2) capability to process and exploit SSA data generated from sensors and catalogues to provide a complete space picture

Theatre of an unprecedented strategic and military competition, space is likely to become a new confrontation frontline in the near future. Easier access to space, increased space debris in orbit, the existence of large space objects capable of offensive actions imply the necessity for Member States to acquire or upgrade capabilities to protect their countries and strengthen their role as sovereign powers.

Specific challenge

The 2018 Capability Development Plan (CDP) points to a shortfall in the Space Situational Awareness (SSA) and early warning domain and identifies the need of an essential capability for securing Member States by preventing natural and manmade threats.

As a prerequisite for further defence cooperation in space, Member States should be able to reach a shared comprehension of what is happening in space.

A European military Space Surveillance Network (SSN) and SSA Command and Control (SC2) system are recognized as peculiar solutions to monitor the space situation and detect threats.

The main challenge is therefore to harmonize a shared military space picture: what its content must be, how to build it, how to share it among Member States according to an agreed information policy, considering that the participating Member States may start from different heritages and may have different interests in space.

The long-term objective of such an extended capability is to achieve a European independence on military SSA, to safeguard European interests in space and rebalance the strategic dialogue on the military SSA topic.

Scope

The proposals, supplementing the civilian objectives of EU SST, must address the development of an advanced space C2 solution to process and exploit SSA data generated from sensors and catalogues in order to provide a complete space picture.

Such solution must take into consideration the following aspects:

- in-orbit assets to monitor and to protect;
- perception of the threats, accidental and intentional, in LEO[40], MEO[41], GEO[42];
- access to a catalogue and to identification data, from patrimonial / partners / trustable-commercial sensors, with different levels of quality and availability;
- SSA centres / C2s, or at least different analysis tools;
- perimeter of responsibilities of ministries of defence and national civil agencies;
- level of participation in the EU SST[43] consortium, which currently provides the main European capability for detection and tracking.

[40] Low Earth orbit.

[41] Medium Earth orbit.

[42] Geostationary Earth orbit.

[43] Space surveillance and tracking.

One of the objective of the proposal must be to agree on and implement the content of a shared actionable recognised space picture.

Targeted activities

The proposals must cover the study, design and prototyping of systems and subsystems, not excluding downstream activities.

The targeted activities must in particular include:

- feasibility studies and system architectural definition of a European SC2 capability. This phase must cover military user requirements analysis, architecture definition, establishment of a programmatic roadmap, preliminary specification of the SSA architecture components (C2, communications, networking);
- formalisation of joint requirements, CONOPS drivers, use cases and architectural drivers, by involving the ministries of defence of the participating Member States to ensure design / operational consistency with other actions, if any, relating to SSA sensors in this call;
- identification and characterization of the relevant sources of data that can contribute to feed the system:
  - patrimonial sources from participating Members States;
  - sources from their institutional partners;
  - sources from trustable / qualified commercial providers.
- definition of CONOPS of the shared part of the SC2, especially:
  - which (and how) catalogue, identification and other types of data should be accessed or shared, between which ministries of defence or other national entity (content, level of processing, mode of access, security;
  - how could these data be further processed and fused, in order to improve their coverage, accuracy, reactiveness;
  - which sensors (or network of sensors) could be accessed and shared, by who, and how;
  - which military services and analysis tools can be shared, *e.g.* to characterize objects, detect abnormal behaviour, evaluate intentional threats, support military operations (ground, air, sea, space).
- experimentation of such joint CONOPS, exchange of data and services under simulated and real conditions;
- agreement on a shared architecture for networking national C2s / SSA centres, sensors (or network of similar sensors), data repositories, including a potential multinational shared area;
- definition of a roadmap for further development, in coherence with national roadmaps of participating Member States;
- overall C2 system architecture and preliminary design of a « network / federation » of enhanced national space operational centres, existing or being developed / planned by participating Member States; definition of interoperability standards, tools, procedures;
- performance engineering regarding cataloguing and identification of space objects on all orbits: completeness, accuracy, reactiveness;
- definition of the overall data model, pertaining to:

  - technical data: orbital and tracking data, identification data (optical and radar imagery, optical and RF spectral data), their auxiliary data, in order to ensure a consistent ingestion, storage, exploitation, share of data within either national C2 or a shared multinational area;
  - operational and supervision data, allowing the national C2s to reflect the operational status of shared sensors.

  This activity must associate the provider of each selected data.
- development of a military SC2 prototype to evaluate architecture performances, help to support concepts of operation with users and support specifications. It must serve to demonstrate how:
  - requests (measurement or access to database) from different national authorities are taken into account and validated;
  - ground sensor planning and tasking is performed;
  - segregation and confidentiality of requests and results are preserved, according to the policy that must be defined, and how the common operational space picture is achieved.
- specification, prototyping and experimentation of structural or critical components, including security management (connectors, *etc.*);
- coordination with other actions, if any, relating to SSA sensors in the same call.

Main high-level requirements

The proposed solution should fulfil the following requirements.

- The networking of C2, and the (potential) multinational / sharing area, together with the set of shared national, partners and commercial data and exploitation services should meet the following requirements:
  - an all-orbit coverage;
  - a detection / tracking / characterization sensitivity compatible with intentionally threatening objects and events;
  - an accuracy and a reactivity sufficient to detect abnormal / threatening / hostile behaviours, with a sufficient reaction time to protect national assets.
- It should include services to efficiently and securely (cyber resilience):
  - connect/interface the national operational centres;
  - exploit and merge all available types of data: orbital, imagery, spectral (optical, RF), traffic dataflow, open sources;
  - plan and task ground based sensors;
  - share access to data and services;
  - edit joint reports;
  - generate shared visualization and space picture;
  - simulate future events, organize joint training and wargaming sessions;
  - support military operations in ground, sea, air, space;
  - guarantee the planning, coordination, and on-orbit synchronization of activities;
  - monitor the mission.
- The security rules of participating Member States should be met, to protect national and shared data and operations;
- It should make appropriate use of national existing / in-development / planned SSA C2's or equivalent assets.

- The European military SSN should allow the national military space operations centres to improve detection and tracking capability of events such as appearance of new objects, close approach of a high value asset by a foreign object.
- The SSN should also allow gathering intelligence on unknown objects through their dynamic behaviour, their optical signature and its variation, and their radio emissions in order to support the evaluation of their mission.
- In this scenario, new applications should be available to complement traditional SST services such as collision avoidance, conjunction analysis, re-entry and fragmentation:
  - pattern of life;
  - anomaly detection;
  - spawning;
  - warning.
- The SC2 should fulfil the following requirements:
  - the SC2 system should provide the capability to detect, track and characterise space objects of military interest as expressed by participating Member States;
  - the SC2 system should be modular and allow each participating Member State to configure / adapt the SC2 at national level to meet its own requirements;
  - the SC2 system should meet the military performance standard in terms of security, RAMS (Reliability, Availability, Maintainability and Safety), response time, resilience, surveillance capacity;
  - the SC2 system should allow processing of data from heterogeneous sources (own SSA sensors, partner sensors (military/civil) as well as commercial sensors, contributor sensors (*e.g.* early warning sensors) or other external data sources);
  - the SC2 system should have an incremental approach for deployment – *e.g.* near-term architecture using existing assets, mid-term architecture using additional new sensors and final architecture should be defined, avoiding any duplication with on-going initiatives at national and Union level (especially EU-SST);
  - the space surveillance interoperable architecture should be scalable by design, easy to extend, able to accommodate an increasing number of users and an increasing capacity;
  - the technical implementation of the data processing and data exchange should foresee the possibility to define data policy rules and should ensure the required level of data security (data integrity, authentication and encryption, *etc.*);
  - SSA data and requests should be exchanged in standardised formats, prioritizing already agreed international standards (if available, such as ECSS or CCSDS[44] TDMs[45] and OEMs[46], *etc.*) for sharing space tracking data and orbital position data or should be agreed amongst partners;
  - SSA information should be exchanged in a cyber-secured and controlled way, ensuring data integrity, authentication and encryption, in respect of the relevant applicable security standards, and allowing exchanges amongst agreed levels of security classification;
  - the SC2 system should provide user interfaces suitable for use by trained personnel within their area of expertise, adaptable and upgradeable;

[44] Consultative committee for space data systems.

[45] Tracking data messages.

[46] Orbit ephemeris messages.

  - a common glossary/documentation of exchanged data, accuracy, underlying models and algorithms should be produced to ensure interoperability. Test procedures should be defined to allow confirmation.

Nota: Member States will maintain full control on their own military SSA capabilities and data, including data dissemination.

Expected impact

- Contribute to the design of an agreed operational and technical SSA capability, shared within associated Member States, with no unnecessary duplication, and providing synergies of data, sensors, services for a mutual benefit;
- Ensure secure and efficient solution of high performance system for specific military end-users, to complement and optimize the use of civilian SST systems;
- Implement the first step of a more efficient share of national capabilities, in order to create a complete SSA capability among Member States with minimal gap;
- Define roadmap allowing the technical transition from the initial operational capability (IOC) to a final operational capability (FOC) European military SC2;
- Make European SSA assets interoperable, enhancing cooperation between undertakings across Member States and achieving a high level performance through overall cost reduction thanks to avoidance of unnecessary duplication.

1.5.2. Topic EDIDP-SSAEW-SSAS-2020 – Enhanced SSA sensors for accurate identification and characterization of existing Geostationary Earth Orbit (GEO) and Low Earth Orbit (LEO) public and private assets

Specific challenge

Space assets and systems have become critical to ensure vital functions of military operations and need to be protected in their outer space environment. Theatre of an unprecedented strategic and military competition, space is likely to become a new confrontation frontline in the near future. Easier access to space, increased space debris in orbit and the existence of space objects capable of offensive actions, imply the necessity for European countries to upgrade or acquire capabilities to protect their space assets and strengthen the potential of their sovereign resources.

Acknowledging these changes to the security environment, and to face them better, the EU Global Strategy for Foreign and Security Policy (EUGS) has started a process of closer cooperation in security and defence. Through this process, based on the identified trends and information gathered from Member States and from the EU Military Committee, security has become today an integral part of the European Space Policy: in 2018, Space Surveillance has been highlighted as a capability gap in the progress catalogue of the EU Military Staff (EUMS) and Space Situational Awareness has been identified as a priority in the EU Capability Development Plan (CDP).

Above the SST sensors provided through the EU-SST initiative, EU military needs cutting edge technology sensors to better identify and characterize the threats (what is it? what is it capable of?) in order to reliably attribute threats.

Scope

The proposals must address the development of future enhanced SSA sensors to improve identification and characterization of existing and future GEO (Geostationary Earth Orbit), MEO (Medium Earth Orbit) and LEO (Low Earth Orbit) public and private assets.

The technologies to be developed may include:

- trajectography for tracking of uncooperative objects;
- sensors for object characterization (*e.g.* photometry, polarization, radar imagery, optical imagery and spectrophotometry, passive RF, passive optical, SLR[47]);
- ground- and space-based instruments.

Targeted activities

The proposals must cover the design and prototyping of systems and subsystems, not excluding upstream or downstream activities.

The targeted activities must in particular include:

- use cases and performance requirements definition; architectural design and solution trade-off; design; build, verification, integration; validation including assessment of performance requirements;

[47] Satellite laser ranging.

- planning and cost estimate related to the following phases, including industrialisation and deployment.

Main high-level requirements

The enhanced SSA sensors should fulfil the following requirements:

- the sensors should have the capability to collect and process space objects' data in order to enable characterisation and identification;
- the best suited set of sensors should be selected, resulting from a gap analysis taking into account identification, characterisation and tracking requirements against the existing technical options (optical, RF, radar, ground and space based);
- the set of developed sensors should be complementary, with the objective to achieve as a whole the performance required to characterise, identify and track all space objects of military interest in terms of availability, field of view, revisit frequency, compatibility with meteorological conditions, target position and target active status;
- the consortium should propose sensor development and test activities to validate the expected performance;
- the sensors should be able to use external data for the planning of measurement collection tasks;
- the sensors output interfaces (measurement data formats, planning interfaces, *etc.*) should respect predefined standards or should be compatible with the exchange formats of the future European military SSA network to facilitate data exchange;
- the sensors design and development should take into account data protection requirements;
- remote operation of the sensors should be feasible;
- commercial/trusted software and hardware components should be used where possible;
- the sensors should provide user interfaces suitable for use by trained personnel within their area of expertise.

Expected impact

- Define roadmap allowing the transition from the initial operational capability (IOC) to a final operational capability (FOC) level consisting of an all-orbit European military SSA system;
- Select/define and de-risk new innovative SSA technologies to support space surveillance capabilities for future architecture increments;
- Contribute to strengthening the European industry in the domain of Space security and help improve its global position through the implementation of innovative technologies along a new European manufacturing value chain.

1.5.3. Topic EDIDP-SSAEW-EW-2020 – Early warning against ballistic missile threats through initial detection and tracking of ballistic missiles before handing over to ground based radars

Specific challenge

The global security environment is evolving with resurgence of great powers competition and nuclear proliferation issues. This topic is an opportunity to initiate the development in Europe of a ballistic missile early warning capability. It aims at developing a European autonomous capability coherent, complementary and interoperable with NATO systems, insofar as Member States rely until now entirely on information provided by a non-EU country distributed through NATO.

Scope

The proposals must address some predevelopment activities of a space-based missile early warning system (SBMEWS).

The proposals must address the stand-alone capabilities of the SBMEWS, the handover to early warning radars and its contribution to the passive and active missile defence, considering all the phases of the missile flight from the launch up to the end.

Targeted activities

The proposals must cover the study of the space-based missile early warning system (SBMEWS) before initiating its further development in Europe.

These activities must in particular include:

- the definition of a set of mission requirements that could be agreed as the basis for a joint development program (see “Main high-level requirements” below);
- the definition of a workable CONOPS, especially showing how the cooperating Member States will get their expected capability;
- the architecture study of the space-based early warning system:
  - considering different candidate architectures in terms of orbits and in terms of level of cooperation;
  - considering stand-alone SBMEWS capabilities;
  - considering handover capabilities to sea-based and ground-based radars;
  - considering SBMEWS contribution to the passive and active missile defence up to the end of the attacking missiles flight;
  - evaluating the candidate architectures regarding capability gaps, availability, reliability, resilience, technological and operational risks and protection possibilities;
  - evaluating the level of answer of the proposed architecture versus the hypersonic missile threat and the evolutions needed to cover fully this threat.
- the feasibility study of the space-based early warning system:
  - including the study of candidate space-based sensors and satellites;
  - including the study of dedicated ground segment architectures which will command the space-based sensors and process the sensors data in order to provide the expected early warning information;
  - including the study of SBMEWS inter-operable C2 architectures which will be in charge of the coordination and the data fusion between candidates space-based

    sensors and in charge of interoperability with early warning radars and missile defence in the scope of the NATO Alliance or between Member States;
  - evaluating the impact of including the hypersonic missile threat on the feasibility of the SBMEWS.
- a programmatic proposal presenting a development plan (highlighting critical path, and, if any, technologies needing anticipatory derisking/predevelopment phase):
  - including a proposal to mature the technologies that would be common to all foreseen architectures, in order to fund their anticipatory derisking, if needed.
- a comparative analysis between the different candidate architectures, the different levels of cooperation and the considered threats (ballistic, hypersonic), including cost aspects.

Main high-level requirements

The Space-Based Missile Early Warning System (SBMEWS) should fulfil the following requirements.

- SBMEWS should fulfil:
  - intelligence mission on Ballistic Missile (BM) test fires, test flights and, if feasible, warhead technology;
  - contribution to territory passive and active missile defence;
  - contribution to theatre passive and active missile defence;
  - observation of space launches.
- SBMEWS should address the ballistic missile threat and space launchers of interest;
  - *Contributing Member States will define (with the support of the study team if needed) the ballistic threat covering missiles class and ranges, missiles' parameters, operational scenarios, trajectories and signatures for space-based sensors design;*
  - *Contributing Member States will define (with the support of the study team if needed) the space launchers of interest covering the types of launchers, launchers' parameters, operational scenario, trajectories and signatures for space-based sensors design*.
- SBMEWS should cover different zones of interest for BM and space launches;
  - *Contributing Member States will define (with the support of the study team if needed) the zones of interest.*
- SBMEWS should insure the surveillance of all BM and space launches from a given geographical zone included in the access zone;
  - The surveillance zone should be selectable into the covered zone;
  - *Contributing Member States will define the maximum dimension of the surveillance zone.* The preliminary maximum dimension of the surveillance zone could include one or several countries.
- SBMEWS should insure its surveillance permanently with a high level of availability;
- SBMEWS should detect BM and space launches from the surveillance zone with a low rate of false alarm and a high probability of detection;
- SBMEWS should measure or estimate the trajectory of all detected launches from their launch up to their ballistic phase and the impact of all detected BM launches;
- SBMEWS should characterize the detected BM and space launchers;
  - The characterized parameters should be discussed with contributing Member States.
- SBMEWS should contribute to update a characterized BM and launchers catalogue;

- SBMEWS should recognize the detected BM and launchers within a known catalogue or identify a new missile or launchers as unknown;
- SBMEWS should contribute to aggressor identification;
- SBMEWS should handover the detected BM and launchers to different early warning sensors;
- SBMEWS should contribute to passive and active missile defence up to the end of missiles' flight;
- SBMEWS should fulfil its missile early warning mission and space launches observation mission in compliance with a real time operation timeline;
- SBMEWS should fulfil its intelligence mission in compliance with an analysis operation timeline;
- SBMEWS should include a space segment and the associated mission and control ground segments;
  - *Contributing Member States will define the location of the mission and control ground segments and of the associated ground stations.*
- SBMEWS should broadcast early warning information to its operational customers and external systems such as GBR (ground-based radars) or SSA (space situational awareness);
- SBMEWS should use secured communication means for internal and external data exchanges;
  - *Contributing Member States will define the level of COMSEC and TRANSEC.*
- The performances of the SBMEWS against hypersonic missiles should be evaluated.

Expected impact

- Setting up the basis of a multilateral development program within the European Defence Fund, giving Member States the autonomous capability of early warning against ballistic (and, if confirmed, hypersonic) missiles;
- Enforce EU contribution to NATO.

1.6. Call EDIDP-MSC-2020 – Maritime surveillance capabilities

The 2018 Capability Development Plan (CDP) points to the need to enhance Maritime situational awareness through a large scope of platforms, sensors, Computer Information Systems (CIS) capabilities. A comprehensive set of sensors and platforms should provide the capability to establish and maintain the maritime situational awareness and level of knowledge required to allow commanders at all levels to make timely and informed decisions. This is key in harbour and littoral protection as well as when maritime high value units are displaced in critical waters. The analysis of long-term trends indicates the need for the ability to collate a range of different ISTAR sensor inputs to detect, track and identify threats across a wide area of operations, including the ability to counter adversary attempts to use low-observability materials, designs and technologies to escape detection.

Proposals are invited against any of the following topics

- **EDIDP-MSC-IS-2020:** Integrated solution to enhance the maritime situational awareness;
- **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) with particular focus on maritime littoral and high sea areas and harbour protection and related critical infrastructure;
- **EDIDP-MSC-CRPS-2020:** Coastal radars and passive sensors with associated relevant networks;
- **EDIDP-MSC-NS-2020:** Maritime surveillance generated by networks of sensors based on fixed and/or semi-fixed unmanned platforms.

Budget

The Union is considering a contribution of up to EUR 20 000 000 to support proposals addressing any of the above-mentioned topics and their associated specific challenge, scope, targeted activities and main high-level requirements.

Several actions, addressing different topics, may be funded under this call.

The Commission will pay particular attention to the civil and dual-use on-going initiatives at Union level to avoid unnecessary duplication.

1.6.1. Topic EDIDP-MSC-IS-2020 – Integrated solution to enhance the maritime situational awareness

Specific challenge

This call intends to develop a modular and interoperable solution to enhance situational awareness and operations in the maritime environment through the development of a multi-sensors and scalable capability to detect, classify, track, and identify threats across a wide area of missions, including the ability to counter adversary attempts to use low-observability materials, designs and technologies to escape detection.

Scope

The proposals must address the development of an integrated solution able to enhance the maritime situational awareness improving detection, classification, tracking, and identification of threats (air, surface and under-water) including the ability to counter adversary attempts to use low-observability materials, designs and technologies to escape detection, with focus on maritime littoral, high sea areas, harbour protection and critical infrastructure.

The proposals must address the following elements:

- a maritime surveillance secure digital platform, able to grant real time info sharing;
- information and data fusion services to merge information and data from different sources, exploiting the large amount of open maritime data;
- detection of anomalous and malicious behaviours, for example by making use of algorithms of artificial intelligence and big data analytics;
- forecast of the evolution of a maritime situation, for example by using predictive algorithms, in support of rapid decision making;
- a multi-sensor, multi-target, common operating picture to enhance situational awareness;
- a collaborative environment among users to share operation data;
- an architecture able to integrate:
  - innovative active and passive sensors with associated relevant networks (*e.g.* sonar, electromagnetic, multi/hyperspectral, video, IR, land-based radar surveillance, effectors);
  - robotics and automated systems for maritime surveillance equipped with different kind of sensors integrated in unmanned surface (USV), underwater (UUV) and aerial vehicles (UAV), both fixed wing and rotary wing;
  - space based sensors such as, but not limited to, AIS[48], optical (including multi/hyperspectral and IR), radar (including SAR), ESM[49] (including ELINT[50]).
- interoperability with heterogeneous systems, including existing systems already available across Europe;
- communication infrastructures to support information management and dissemination;
- Man-Machine teaming approach based on user experience to provide ergonomic, customisable and layered interface to the operators.

[48] Automatic identification system.

[49] Electronic support measures.

[50] Electronic intelligence.

Targeted activities

The proposals must cover the study and design of the proposed solution, not excluding downstream activities.

The targeted activities must in particular include:

- feasibility study, including CONOPS, specifications, detailed requirements reviews and architecture definition. Requirements analysis for new sensors will be part of the study;
- detailed design, including the Preliminary Design Review (PDR) and the Critical Design Review (CDR) of the proposed solution.

The proposals could also include the development of small-scale technological demonstrators, in order to support decision making during design phase.

Main high-level requirements

The proposed solution should:

- be based on a modular approach in order to mature technologies, improve system and subsystem capabilities and to interface third-party systems;
- have an open and secure architecture able to grant real time info sharing, and enabling cooperation between military and civilian actors (dual use as hydrographic data, civil authorities operational data, *etc.*);
- have a design based on the federation of national systems, through interoperable nodes and adaptors, in order to increase the EU maritime situational awareness;
- have a guaranteed resilience, ensuring an adequate level of cyber protection, monitoring and incident management;
- guarantee a proper bandwidth, latency and other connectivity parameters to ensure proper exchange of data in all scenarios from peace time to war time through grey zone;
- detect anomalous or malicious behaviour, for example by implementing artificial intelligence algorithms and big data analytics;
- integrate all types of innovative sensors, including passive sensors capable of intercepting and identifying emissions in a congested electromagnetic spectrum (coming from both cooperative and non-cooperative sources);
- address integration of deployable solutions, consistent with available maritime bandwidth;
- provide advanced user interfaces supporting the maritime organization operators in all their operational, technical and training needs;
- support dedicated training configuration to assure an effective “train as you fight” approach.

Expected impact

- Reduce the workload, speed-up the processes and support operators;
- Provide a solution able to integrate platforms and sensors from Member States and EU agencies and bodies;
- Improve interoperability, information sharing and collaboration among end users;
- Define a common interoperable security and defence system of systems architecture;

- Contribute to the strategic autonomy of the EU.

1.6.2. 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) with particular focus on maritime littoral and high sea areas and harbour protection and related critical infrastructure

Specific challenge

The EU has an increasing need of geospatial information for its decision-making processes.

In this field, the use of advanced satellite-based observation assets leads to a significant increase of the operational performance of current systems.

However, the development, launch and operation of a satellite for observation purposes require a large investment and a long development timeline. In this context, platforms based on small satellites (less than 100 kg) and the use of high-performance optical observation equipment could be a suitable approach providing they can meet the right resolution, (re)visiting time and operational requirements.

Scope

The proposals must address the development of a small satellite mission for maritime surveillance, including all mission segments (*i.e.* flight, ground, launch and user segments).

The proposals must in particular address the technology issues relating to:

- mission design guidelines. Outline the main input parameters and variables to define the suitable mission for the maritime surveillance requirements;
- system engineering and integration procedures for the different components of the satellite depending on the designed mission. Special attention should be given to the communication electronics, as well as the optical payload processing unit;
- ground segment and operation requirements depending on final user surveillance needs. For example, number of images per target, revisiting frequency, *etc.*;
- image processing aspects depending on the mission, assigned orbit and specific surveillance requirements;
- satellite agility to enable the continuous acquisition of target locations, namely maritime borders or coastlines.

Targeted activities

The proposals must cover the study and design of a small satellite mission for maritime surveillance, not excluding downstream activities.

The targeted activities must in particular include:

- a feasibility study and the preliminary requirements, determining and examining the mission objectives:
  - Mission Definition Review (MDR). Having obtained the mission statement, a certain mission for a maritime border or coastline must be proposed as a use-case for the small satellite system;

  - Preliminary Requirements Review (PRR). Preliminary technical specification of the mission defined in the MDR phase and confirmation of the technical and programmatic feasibility of the system and operations concept;
  - Systems Requirement Review (SRR) consolidating technical specifications at system level for the defined mission in the MDR phase. The PRR and SRR imply the identification of some lead users to state and validate such requirements.
- the design phase. Providing the mission and the system requirements are defined, the system design must be subject to two consecutive activities:
  - Preliminary Design Review (PDR). The proposed design will be validated against the established system requirements for the proposed mission;
  - Critical Design Review (CDR). This activity will demonstrate that the system's design can be implemented into a functional prototype and the subsequent industrial scale-up.

These activities must also include:

- the analysis of an integrated and synergic approach for the use of small satellites versus traditional EO satellites, with focus on SAR-Optical federation for IMINT, not excluding SIGINT solutions;
- the capability to operate an optical payload providing resolutions about 1 m or below in panchromatic and RGB[51], the electronics in charge of the on-board image processing (*i.e.* super-resolution algorithms), thermal and power control, as well as the mission design including ground segment and communication requirements;
- the selection criteria for the adequate launcher and operational requirements for the chosen orbit(s).

Main high-level requirements

The proposed work should fulfil the following requirements:

- identification of the opto-mechanical requirements for the optical payload taking into account the constraints of using a small satellite platform (less than 100 kg in total);
- selection of the adequate electronics for the detectors (*e.g.* CMOS technology) and the on-board control and processing (*e.g.* FPGA or GPU-based systems);
- definition of the alignment and calibration procedures of the camera for future prototyping and industrial scale-up;
- specification of the power unit and the corresponding control system, following the requirements of the chosen mission operations concept;
- specification of the thermal control requirements for the system considering the selected orbit and mission conditions (*e.g.* passing time and time of observation over target);
- selection of the orbit and the maximum tilt off-nadir for the satellite, including the strategy to track a coastline or maritime border. The camera FOV / FOR (Field of View / Field of Regard) will be requirements to be addressed for the chosen orbit;
- analysis and requirements for attitude control actuators of the satellite platform. In this mission it implies specific requirements (*e.g.* for the reaction wheels to be used under the mission conditions);

[51] Red, green and blue.

- star tracker requirements should be also considered regarding the high satellite attitude knowledge and pointing precision needed to meet the operational requirements;
- specific requirements for on-board image processing, including super-resolution algorithms and compression of the resulting images for downloading;
- the requirements for the communication electronics and antennas will be stated for a certain download channel, assuming the system will be operating under high-throughput conditions;
- downlink requirements should be carefully taken into account, including the design of the ground segment (*e.g.* number and location of the ground stations), satellite TTC (Telemetry, Tracking and Command) and operation and post-processing of the image to meet the surveillance awareness requirements;
- analysis and requirements for automatic data processing to enable maritime borders and coastlines monitoring, by taking advantage of the experience gathered by EU industry in providing services to the market;
- analysis of a federation oriented approach between small and traditional satellites;
- the overall system and software architecture will be defined to set the base for future ISVV (Independent System/Software Verification and Validation), as part of the scale-up of the system;
- the estimate of the small satellite lifetime should also be provided taking into account that some of the selected components are expected to be “commercial-off-the-shelf”. De-orbiting should comply with the accepted standards.

The system architecture of the small satellite for maritime surveillance mission should take into consideration all necessary future elements for full capabilities deployment, and in particular:

- the system operation under constellations for the specific mission to be defined. This will lead to additional requirements for the system’s data downlink and operation;
- the type and features of the launchers to be considered to meet the coverage and revisit requirements. The selected orbits and targets will be a key factor since some orbit deployment strategies may require a dedicated launch or propulsion, with the corresponding cost implications;
- the development of applications for agile processing of the images downloaded in a quasi-real time scheme. The computing capacity could grow in a significant way depending on the amount of information and the final users’ demand; hence, AI and Big Data processing techniques could be also included in this analysis.

Expected impact

- Development of critical capabilities for EU CSDP;
- Efficiency improvement of the European defence;
- Reinforcement of the interoperability of EU Member States armed forces and security agencies (*i.e.* FRONTEX);
- Improvement of the coordination and cooperation in investment, capabilities development and operative availability;
- Enhancement of the competitiveness and innovation capacity of the EU defence industry;
- Reduction non-EU dependencies regarding land and maritime surveillance;

- Improvement of GEOINT satellite-based capabilities, by integration of small platforms;
- Fostering the development of EU launchers industry for small payloads.

1.6.3. Topic EDIDP-MSC-CRPS-2020 – Coastal radars and passive sensors with associated relevant networks

Specific challenge

EU requirements for increased maritime surveillance calls for a capability to detect and track stealth targets and targets difficult to be detected by conventional radars, without running a risk of being detected and jammed. In this regard, the solution of passive bistatic/multistatic radars is considered as a promising alternative.

Additionally maritime surveillance should take into account archipelago, harbours and coastal urban areas, the surveillance of which requires the deployment of a dense network of sensors. Passive radars are by nature of lower cost because they do not include high power transmitters and the associated modules (*i.e.* high voltage power supplies, cooling circuits, *etc.*). Therefore, it is possible to comply with the above mentioned requirement by using a large number of passive radars which will exploit existing RF transmissions (transmitters of opportunity).

Scope

The proposals must address the development of a passive, highly performant, resilient, reconfigurable and deployable radar system, with respect to multiple defence application scenarios and diverse target specificities.

The proposals must address at least the following points:

- detection of sea and air targets at all altitudes. Current commercial solutions respond only to lower tier targets;
- efficiency assessment of candidate transmitters of opportunities;
- capability to fuse detected cues using different type of illuminators;
- demonstration of the capability of operation in network (multiple sensors exploiting one common or multiple transmitters of opportunity);
- where possible, use of COTS technologies currently available from European supply chains;
- development of SDR[52] modules tailored for PCL[53] technology;
- assessment of innovative antenna configurations;
- reconfigurable technologies to achieve long term adaptability and application migration.

Targeted activities

The proposals must cover the study, design, prototyping and testing of the proposed solution, not excluding downstream activities.

The targeted activities must in particular include:

- feasibility study, CONOPS definition, technology/system specification, detailed requirements review (DRR), analysis of possible extensive cognitive capabilities;

[52] Software design radio.

[53] Passive coherent location.

- detailed design of the technology/system, including the Preliminary Design Review (PDR) and ending with the Critical Design Review (CDR);
- development of small-scale technological demonstrators, in order to support decision making during the design phase of the final prototype;
- development, testing and validation of the final prototype system.

A detailed planning of subsequent project phases must also be generated, including the identification of implementation priorities according to operational needs of the EU and its Member States.

Main high-level requirements

The proposed system should fulfil the following requirements:

- detect sea and air targets at all altitudes, including RPAS and low observable targets;
- measure target's bearing, distance and speed;
- assistance to the point / areal air defence of navy units and coastal infrastructure;
- provide limited cognitive capabilities (*i.e.* eliminating clutter and multipath);
- improved CFAR[54] responses within a multistatic network for the detection of low observable / low RCS[55] targets;
- develop target classification database based in bistatic target RCS and target behaviour in the range-Doppler map.

Expected impact

- Develop critical technology enablers for counter low observable air and sea targets including RPASs and aircraft flying hidden by geographical profile;
- Reinforce interoperability between EU Member States' armed forces and reinforce cross force protection;
- Improve maritime situational awareness for the security of the EU and its Member States;
- Increase EU technological sovereignty (in terms of hardware and software) in a critical defence area.

[54] Constant false alarm rate.

[55] Radar cross section.

1.6.4. Topic EDIDP-MSC-NS-2020 – Maritime surveillance generated by networks of sensors based on fixed and/or semi-fixed unmanned platforms

Specific challenge

Current unmanned systems used for maritime surveillance are unable to fulfil the need for persistence, permanence and cross-domain situational awareness at low cost and reduced staffing. There is, therefore, a need for a new type of asset that will take advantage of a remote decentralized distributed sensors and C3[56] network architecture, which will decrease the need to deploy high value manned assets to perform maritime surveillance and deliver persistent and permanent holistic maritime situational awareness.

The type of asset must be able to accommodate both existing and emerging sensors and other required technologies in a cost effective and operationally robust way. A key requirement for this new type of assets is to be able to perform long-range cross-domain maritime surveillance. In addition, this type of asset must be floating, thus semi-fixed, able to be re-deployed and thus reconfigure the network's spatial arrangement within the EU offshore areas of interest.

Scope

The proposals must address the development of a network of floating (semi-fixed) unmanned and autonomous platforms able to support the housing and simultaneous operation of a broad range of maritime surveillance assets and capabilities.

The network of floating platforms must be able to provide holistic and persistent situational awareness within the maritime domain. In particular, the floating platforms must be able to perform data exchange and energy recharge actions for a variety of UxVs while being able to securely and robustly communicate with C3 centres and to accommodate various types of radars, including but not limited to monostatic, bi-static and multi-static configurations facilitating beyond the horizon capabilities. Moreover, the platforms must be able to support electro-optical sensing devices as well as hydroacoustic arrays (including sonars) and other underwater sensors (*e.g.* magnetic anomaly detectors). Additionally, it has to provide secure housing facilities for a number of UxVs. The individual platforms, as well as the network as an integrated system of systems, must accommodate sufficient means for self-defence against relevant threat vectors.

Targeted activities

The proposals must cover the study and design of the proposed solution, including partial testing of technology components, not excluding downstream activities.

The targeted activities must in particular include:

- the study of a network of at least three platforms able to satisfy the high-level operational requirements;

[56] Command, control and communications.

- the design at the level of detailed definition of a platform type of the network for a future prototype trial, including CFD[57] simulations and tank tests of the proposed platform;
- the testing of the docking and undocking component for the UUVs to the platform may be tried.

Main high-level requirements

The following requirements should be fulfilled by the proposed network of platforms and the individual platforms.

The network should:

- consist of several platforms (floating structures);
- have the capability to utilize different classes of platform types in respect to functionality and operational capabilities;
- be capable of being redeployed in areas with similar sea state and sea bed characteristics;
- be able to securely intercommunicate and communicate to command and control centres as well as operational centres;
- be capable to securely and robustly communicate with relevant C3 infrastructure and various operational hubs;
- have the capability to serve as a link between C3 infrastructure, operational hubs and various assets in the area of responsibility;
- have the capability to operate in electromagnetic and cyber contested environments;
- have the capability to provide passive and active self-defence means and measures at local scale;
- be scalable, modular and upgradable;
- have the capability to retain operational efficiency even with a reduced number of performing platforms.

The platform should:

- accommodate capabilities that support cross domain situational awareness (*i.e.* underwater, surface and air);
- have an exposure surface of minimum RCS possible;
- have the capability to maintain less than 5 degrees of inclination in severe sea state conditions at least at 95% of operational time;
- have the capability to be deployed in areas with deep and very deep waters (more than 500 m);
- have the capability to accommodate various types of sea bed conditions encountered in the Mediterranean, the Atlantic, the Baltic and the North Sea;
- have the capability of hosting vertical take-off UAVs to perform surveillance and reconnaissance missions;
- be able to serve UxVs as a hub by providing data exchange and recharge services;

[57] Computational fluid dynamics.

- have the capability to accommodate and integrate a variety of sensors (*i.e.* various types of radars, sonars, electro-optical, hydro acoustic and magnetic anomaly detecting devices, *etc.*);
- have the capability to adopt a plug and play design for mission specific modules;
- have the capability to interchange mission specific modules in a timely manner;
- be able to accommodate masts at least of 40 meters height above sea level serving both as antennas and support infrastructure for various sensors;
- be energy autonomous for 6 months of continuous operation in terms of on-board systems, on-board sensors and hosted assets;
- have the capability to integrate and deploy a variety of passive and active, self-defence means and measures.

The network and individual platforms should accommodate and facilitate the enforcement of the relevant EU doctrines.

Expected impact

- Develop a critical enabler for CSDP (Common Security and Defence Policy) operations and missions in the maritime domain;
- Improve maritime situational awareness for the security of the EU and its Member States;
- Facilitate defensive naval operations in any operational context;
- Support enhanced joint operations situational awareness (underwater, surface and air);
- Provide advanced early warning capabilities for joint operations commanders;
- Reduce reliance on manned assets in the context of maritime surveillance;
- Contribute to EU strategic autonomy.

1.7. Call EDIDP-NGPSC-2020 – Upgrade of current and development of next generation ground-based precision strike capabilities

The 2018 Capability Development Plan (CDP) identifies the need for the upgrade of current and development of next generation of direct and indirect fire support capabilities for precision and high efficiency strikes, including ammunition and fire control systems.

Proposals are invited against any of the following topics

- **EDIDP-NGPSC-LRIF-2020:** A Platform for long range indirect fire support capabilities;
- **EDIDP-NGPSC-PGA-2020:** Programmable and guided ammunition.

Budget

The Union is considering a contribution of up to EUR 7 000 000 to support proposals addressing any of the above-mentioned topics and their associated specific challenge, scope, targeted activities and main high-level requirements.

Several actions, addressing different topics, may be funded under this call.

The Commission will pay particular attention to existing and on-going developments within the Union to avoid unnecessary duplication.

1.7.1. Topic EDIDP-NGPSC-LRIF-2020 – A Platform for long range indirect fire support capabilities

Specific challenge

Due to the evolution of the defence context in Europe, land forces need the ability to operate in a high intensity threat environment, facing potential technically advanced adversaries. In this context, associated firepower to protection of forces like artillery capabilities need to have their range, precision and efficiency improved.

Scope

The proposals must address the development of an enhanced European artillery through the upgrade of current and development of next generation of indirect fire (IDF) artillery systems (both gun self-propelled systems and rocket launchers).

Targeted activities

The proposals must cover the study and design of the proposed solution, not excluding downstream activities.

Main high-level requirements

Precise requirements will be defined together with the participating Member States during the study phase.

The IDF artillery solution to be designed should fulfil the following requirements:

- able to reach long ranges (minimum 60 km for gun self-propelled systems, minimum 200 km for rocket launchers) with an accurate guidance;
- capable to fire conventional and guided long-range and programmable precise ammunitions (155 mm shells for gun self-propelled systems);
- interoperable with EU Member States and NATO countries;
- able to perform deep strikes;
- able to strike at counter-fire and at high-payoff targets;
- feature accurate and robust Position, Navigation and Timing (PNT) performances in order to operate under denied or degraded GNSS environment;
- have a high level of automation for improved performances and crew reduction;
- have an autonomous and fast resupply system to reduce vulnerability;
- have optimized life cycle costs, maintenance ability at battery level, durable artillery guns vis-à-vis longer ranges, and be reliable;
- have a high level of reliability in all weather conditions;
- include a command and control system:
  - able to provide command and control of the whole platform;
  - allowing the integration of the system into European indirect fire capabilities;
  - compliant with either national and NATO standards;
  - based on an open architecture able to reduce the life-cycle process and enhance the integration phase;
  - based on a modular architecture in order to easily adapt to new effectors for precision strike.

Expected impact

- Support to the security and defence interests of the EU;
- Contribution to the European industrial autonomy, avoiding any dependence on third non-European countries;
- Contribution to increased interoperability and potential European standards;
- Reduction, through commonality and mass production, of the acquisition and life-cycle costs for each Member State;
- Competitiveness due to new market opportunities;
- Reduction of the cost of European military missions.

1.7.2. Topic EDIDP-NGPSC-PGA-2020 – Programmable and guided ammunition.

Specific challenge

The objective of this topic is to pave the way for a European independent solution providing 155 mm 52-calibre artillery with very long range, high precision and heavy payload ammunition. The proposed solutions must address future challenges such as increasing action range beyond the range of potential near-par threats, decreasing dramatically collateral damages, operating in a GNSS-denied environment, providing ammunition with an improved targeting capability and potentially in-flight retargeting to provide maximum flexibility and safety of use for friend troops.

Therefore, the contemplated future ammunition will bring several advantages over current limited and partially non-sovereign solutions.

Technologies and functions developed under this topic will be also available for rocket artillery since they address the same challenges regarding precision, range, effectiveness and operation on a GNSS-denied battlefield.

Scope

The proposals must address the development of a very long range (> 60 km), high precision and heavy payload ammunition.

Deliverables are expected within 24 months from the signature of the grant agreement.

Targeted activities

The proposals must cover the study and design of the proposed solution, not excluding downstream activities.

The targeted activities must in particular include:

- feasibility studies encompassing: terminal effect rough assessment, ammunition architecture choices regarding propelling system, projectile and warhead type, interface with gun and artillery system integration;
- preliminary design of a complete ammunition;
- the provision of a roadmap for subsequent development phases (*e.g.* functional demonstrator to be tested in a proven 155 mm 52-calibre artillery and available technologies for future rocket artillery).

Main high-level requirements

The ammunition should fulfil the following requirements:

- interoperability between EU Member States and NATO countries. Especially, the 155 mm ammunition should be compliant with the Artillery JB MOU[58] and be tested in a proven 155 mm 52-calibre artillery;
- every technology and component developed to address the above challenge should be capable of being integrated into an artillery rocket. Therefore, technical specifications at

[58] Joint ballistic Memorandum of understanding.

all stages should encompass the two categories of ammunition. It is expected that the stress put on compactness and resistance to the extreme thermo-mechanical environment of a 155 mm artillery shell will enable technologies and components to withstand the environment of an artillery rocket;

- the ammunition should provide a terminal precision below the 10 m (CEP@50) range, in all weather conditions. It will be flight-guided by GNSS and/or inertial measurement unit and/or any cost-effective means, and it will resistant to jamming in GNSS-denied environment over the battlefield thanks to Position, Navigation and Timing (PNT) solution or any other means;
- the ammunition guidance and navigation should be GPS and Galileo compatible, without creating any non-EU restriction of use;
- terminal guidance should be based on SAL[59] and/or IIR[60] / imagery system or any other solution to be affordable and effective against moving or stationary targets;
- the ammunition (shell or rocket) should be programmable before firing to realize the mission, with minimum interference with the gun system as far as the 155 mm is concerned. In-flight re-targeting capability (including mission change and/or a mission abort when needed) should be assessed for the different categories of ammunition.
- ammunition safety of use should be as high as possible, as per the best standards related to life duration and insensitiveness to aggressions. Especially, compliance with NATO STANAG 4439 (related to insensitive munition) and STANAG 4187 (related to safety) should be ensured as far as possible;
- high robustness against jamming;
- regarding range, the ability to attack the enemy in depth, to strike at counter-fire and target high value targets is a should. The highest possible range should be sought;
- in particular for the 155 mm, the purpose is to double the standard range of most existing 155 mm 52-calibre artillery, *i.e.* to raise it from approximately 40 km to 80 km or more. A minimum threshold of requirement is 60 km;
- such extended range should be achieved for deep fire missions with high accuracy, as well as to provide area effects;
- the ammunition warhead should be effective against soft targets, light vehicles, small buildings, and should be capable of incapacitating armoured vehicles. Accordingly, warhead and terminal effect should be optimized (scalable effect depending on target objectives); the use of insensitive explosive (HE IM[61], MURAT 1*[62]) is requested, as far as possible. When not possible, this has to be justified;
- terminal phase characteristics (*i.e.* fuse and warhead architecture) should be determined according to the kind of effect considered. Typical options for activation are impact, delayed impact and predefined altitude;
- performances should be achieved without modifying the requirement of existing European artillery rocket launchers and 155 mm 52-calibre artillery guns.

Note: International standards as JB MOU covers only basic interface characteristics. Further safety analysis and testing will be required ahead of in-servicing, to be planned in a later phase out of the current scope. The approach regarding rockets is similar.

[59] Semi active laser.

[60] Imaging infrared.

[61] High explosive insensitive munition.

[62] 1 star marked « Munitions à risques atténués ».

Expected impact

- Availability of an affordable and cost effective artillery ammunition, with performances beyond any current solution;
- Contribution to the strategic autonomy of the European Union and of its industrial base: sovereign key technologies will allow this cutting-edge armament to be used on the battlefield regardless of non-European technologies, components and services, whenever and wherever required, and will provide complete freedom of exportation within the frame of the licenses which may be granted by European bodies and/or participating countries;
- Improved competitiveness due to new market opportunities;
- Reduction, through commonality and mass production, of the acquisition and life-cycle costs for each Member State;
- Contribution to increased interoperability and potential European standards;
- Reduction of the logistic burden of European military land forces;
- Reduction of the cost of European military missions.

1.8. Call EDIDP-GCC-2020 – Ground combat capabilities

The evolving operational environment requires the development of next generation and the upgrade of current armoured platforms with improved robustness, agility, versatility and interoperability with next generation systems and future unmanned systems. A comprehensive combination of land systems should contribute to the capability of land manoeuvre in the joint operational environment to gain positional advantage in respect to the adversary.

Proposals are invited against the following topic

EDIDP-GCC-2020: Development of next generation and upgrade of current armoured platforms, including those able to operate in extreme climates and geographical environments.

Budget

The Union is considering a contribution of up to EUR 9 000 000 to support proposals addressing the above-mentioned topic and its associated specific challenge, scope, targeted activities and main high-level requirements.

Several actions may be funded under this call.

Specific challenge

The evolving operational environment requires the development of next generation and the upgrade of current armoured platforms with improved robustness, agility, versatility and interoperability with next generation systems and future unmanned systems.

Scope

The proposals must address the upgrade of current or the development of next generation armoured platforms, in particular addressing Main Battle Tank (MBT) or Infantry Fighting Vehicle (IFV) or Armoured Personnel Carrier (APC) or other light armoured vehicle, or developing and integrating modern and upgraded systems, subsystems or sensors into existing platforms and/or payloads improving significantly their performance.

Targeted activities

The proposals must cover the study of the proposed solutions, not excluding downstream activities.

The targeted activities could in particular include:

- the collection and definition of concept of operations (CONOPS);
- a feasibility study for the possible concept and technical solutions which fulfil the given high level requirements, including a Detailed Requirements Review (DRR);
- the detailed system specification (*i.e.* SSS[63] and SSDD[64]);
- the high-level design of the selected concept;

[63] Sub-system specification.

[64] Sub-system design description.

- the detailed design of the system, including a System Requirement Review (SRR), a Preliminary Design Review (PDR) and Critical Design Review (CDR);
- the elaboration of a demonstrator;
- the benchmarking/testing of the demonstrator platform against the requirements.

Main high-level requirements

The proposed solution should fulfil the following requirements:

- all systems and subsystems should have a system of systems approach including open architecture concepts (*e.g.* NATO Generic Vehicle Architecture (NGVA));
- systems should improve logistic footprint and security of supply;
- cyber security should be implemented in all layers of hard and software control functions.

In case of development of new or upgrade of existing tactical platforms/payloads, the proposed solution should also fulfil the following requirements:

- systems should provide a substantial improvement of mobility including possibility to combine high level tactical and operational mobility with minimum performance degradation due to extreme environmental condition and type of terrains as defined in the relevant standards (*i.e.* NATO STANAG 2895);
- the system should be capable of performing their missions, by day, night and under chemical, biological, radiological and nuclear (CBRN) conditions;
- the system should be optimized to carry out different role tasks according to their specific performance criteria (*e.g.* troop carrier or firepower);
- the system should comply with the maximum acceptable weight and overall dimensions mandated by transportability requirements and constraints of EU roads, railways, tunnels and bridges; air transportability/drop should also be taken into account; system should also have the capability of crossing water obstacles;
- systems should have high modularity, different versions from one base platform, modular protection levels and taking into account relevant future threats within the operating environment;
- the system should enable low total cost of ownership, including acquisition and lifecycle costs; systems efficient operational lifecycle for new systems should be at least 30 years;
- system should enable payloads capability, low detectability and low signature;
- systems should be prepared for unmanned/optionally manned operations and should be based on innovative and efficient environmental/logistic footprint reducing dependence on fossil fuel.

In case of performance improvement of existing platforms/payloads by development and integration of modern and upgraded systems, subsystems or sensors, the proposed solution should also fulfil the following requirements:

- state-of-the-art system, with modern and intuitive user interfaces (yet compatible with the existing best practices in the field) allowing a fast learning curve;
- system should substantially increase situational awareness of platforms;

- systems should minimize detection and response time to toward entities/potential threats and/or enhance main weapons' effectors (*e.g.* through the use of sensors);
- system should also support effective use of communications, covering also tactical levels. The system should operate in a full IP communication network that should be able to seamlessly use any available transmission mechanism.

Expected impact

- Rebuild a credible deterrent in terms of land combat capability, by introducing in the shortest time a significant number of advanced armoured combat vehicles;
- Introduce new innovative (spin-offs) vehicle technologies and capabilities that can be adopted to other vehicles/platforms/layouts;
- Increase EU industry capability to produce new highly innovative vehicle systems;
- Provide solutions that solves future capability needs of several Member States with maximum commonality and modularity;
- Provide vehicle solutions, which have a reduced environmental/logistic footprint;
- Establish European business consortium able to offer competitive solutions for global market;
- Decrease dependence from non-EU technologies and products.

1.9. Call EDIDP-ACC-2020 – Air combat capabilities

Air superiority is a key factor for European armed forces to defend European territory and citizens as well as to respond in more remote geographical areas. The 2018 Capability Development Plan (CDP) highlights the importance of developing the suppression of enemy air defence capability, the need to integrate and combine manned and unmanned platforms in a larger operational system, the need for airborne electronic attack capabilities, the ability to carry out deep strikes as well as upgrading or developing next generation combat helicopters, including self-protection systems for fixed and rotary wing aircraft. The 2018 CDP long-term capability analysis also identifies the need to ensure overmatch in air-to-air engagements, including against fully autonomous Unmanned Combat Air Vehicles (UCAVs) and to penetrate adversary-controlled airspace to achieve the desired air supremacy.

Proposals are invited against any of the following topics

- **EDIDP-ACC-CH-2020:** Upgrading or developing next generation combat helicopters;
- **EDIDP-ACC-SPS-2020:** Self-protection systems for fixed and rotary wing aircraft;
- **EDIDP-ACC-3MACS-2020:** EU multiplatform mission management capabilities for air combat systems.

Budget

The Union is considering a contribution of up to EUR 22 000 000 to support proposals addressing any of the above-mentioned topics and their associated specific challenge, scope, targeted activities and main high-level requirements.

Several actions, addressing different topics, may be funded under this call.

1.9.1. Topic EDIDP-ACC-CH-2020 – Upgrading or developing next generation combat helicopters

Specific challenge

Combat helicopters are key equipment in the joint operational environment to gain positional advantage in respect to the adversary.

The evolving operational environment, becoming more and more demanding both for the platform and for the crew, requires the development of next generation and the upgrade of current combat helicopters with improved robustness, agility, versatility, level of flight automation and interoperability with next generation systems and future unmanned systems.

Scope

The proposals must address the development of an advanced collaborative system for increased mission efficiency of manned platforms combined with unmanned platforms by means of a newly developed generic Manned-Unmanned Teaming (e-MUM-T) system. The system will allow the manned and unmanned platforms to be able of performing operational missions, which include the helicopter and the UAV, in demanding scenarios.

The proposals must consider several key aspects:

- robustness of the system to operate in several environment (denied, enemy defence strategy…);
- agility of the system to cope with operational mission change/evolution;
- versatility of the generic platform to ensure compatibility with different configurations;
- interoperability in term of data exchange between UAV and helicopter which will allow data fusion and combined mission operational decision;
- independence of the systems relative to the used platforms;
- autonomy support of the manned platform at different levels;
- autonomy of the platforms to improve operations while maximizing the survivability and efficiency of the squadron in operation.

Targeted activities

The proposals must cover the study, design, prototyping and testing of e-MUM-T systems.

The targeted activities must in particular include:

- study:
  - feasibility studies;
  - definition of the Concept of Operation (CONOPS).
- design:
  - systems/equipment specification;
  - Detailed Requirements Review (DRR);
  - architecture definition;
  - preliminary design.
- prototyping and demonstrations (flight testing).

Main high-level requirements

The proposed solution should fulfil the following requirements:

- the collaborative system should be developed to achieve compliance with military standards and civil regulation for airworthiness and mission efficiency requirements directly applicable to the teaming system;
- the collaborative system should reduce the overall crew workload and develop autonomy of operation for manned and unmanned platforms;
- a generic e-MUMT system compliant to the above CONOPS should be developed and applied to one or more specific configurations (pending selected helicopter and UAV configuration). The design of an EU standard interface protocol should be developed;
- the e-MUMT system should take into account the 5 levels of interoperability (LOI) as defined in NATO document STANAG 4586 and add 2 new LOI (full autonomous level, semi-autonomous level);
- the system should include:
  - a mission planning system integrating the e-MUMT required sub-system functions into an existing mission planning system;
  - a remote control station adaptation to ensure UAS nominal operating mode in a “permissive” environment;
  - the UAV platform, integrating the e-MUMT required sub-system functions and equipment into an existing UAV (UAV adaptation);
  - the helicopter platform, integrating the e-MUMT required sub-system functions and equipment into an existing helicopter (helicopter adaptation);
  - advanced flight control actuation with new actuators and integration into existing flight control system;
  - the e-MUMT mission management sub-system as a stand-alone system;
  - light and compact crew/vehicle interface/Human Machine Interface (HMI).
- the e-MUMT system should demonstrate the achievable performance:
  - through ground simulation of several operational scenarios;
  - through demonstration flight tests on one operational scenario.
- the e-MUMT system should be based on civil certifiable solution adapted to military environments/requirements and should support the certification and interoperability standards that will support the development of new products and the operations in Europe and within NATO;
- the e-MUMT system should be able to operate in a degraded environment (GNSS denied service, jammed communication);
- the e-MUMT system should support autonomy modes: flying on predefined route or on route modified in real time by the helicopter crew or by the on-board solver route module;
- the e-MUMT system should support versatile UAV or helicopter configurations;
- the e-MUMT system should have an open modular architecture to ease the integration of new functions without impacting the certification of the certified system;
- the architectural solutions should allow the integration on existing platforms.

Expected impact

- Assist the helicopter crew in a more and more complex environment;
- Increase the efficiency of a manned/unmanned squadron over an operational theatre;

- Increase mission efficiency in the upcoming conflicts, through usage of teamed aircraft, sharing dedicated parts of the collaboration.

1.9.2. Topic EDIDP-ACC-SPS-2020 – Self-protection systems for fixed and rotary wing aircraft

Specific challenge

Innovative self-protection systems are crucial to efficiently tackle a wide range of threats and increase the platform survivability in a hostile environment.
One key challenge is to develop a European self-protection system compact enough to be integrated even on a helicopter and capable to counter current and future more agile threats.
The other is to maintain the affordability of the self-protection system while its complexity increases.

To increase the survivability of the platform, the new-generation of self-protection system must be able to detect threats, improve response time and increase the efficiency of the countermeasure.

A new compact European self-protection system should also set the example forward and use, develop and improve standards for subsystem integration.

Overall system management

Delivering efficient sensing and effective reaction capability in the complex, contested and congested battlespace of the future will require a very integrated approach inside a platform and between platforms equipped with a new-generation of self-protection system. At the core of this integration is the electronic warfare (EW) manager that is providing coordinated management and control of the self-protection system's subsystems.

Scope

The proposals must address the development of a complete, advanced and versatile self-protection system for fixed (transport mission) and rotary (combat and transport missions) wing aircrafts self-protection system.

The proposed solution must include the following subsystems:

- Missile Warning System (MWS);
- Radar Warning Receiver (RWR);
- Counter Measure Dispenser System (CMDS);
- Expendable Active Decoy (EAD);
- Directed InfraRed Counter Measure (DIRCM);
- EW manager;
- Laser warning receiver;
- Other counter measures.

Hard-kill solutions can also be considered.

Targeted activities

The proposals must cover study and design, not excluding downstream activities, of the proposed solution.

The targeted activities must in particular include:

- feasibility study including definition of the concept of operations (CONOPS), system specification, Detailed Requirements Review (DRR) and architecture definition;
- detailed design of the system, including the Preliminary Design Review (PDR) and potentially the Critical Design Review (CDR).

The proposals may also include the development of technological demonstrators, with the involvement of platform integrators, in order to support decision making during the design phase.

A detailed planning of the subsequent development phases must be generated, including the identification of implementation priorities, according to operational needs of the Union and its Member States.

Main high-level requirements

The system should fulfil the following requirements:

General

- The system should provide the following main functions:
  - situation awareness;
  - threat detection and warning alert;
  - threat classification and identification;
  - counter-measures actions with and without a man in the loop.

Common requirements

- The system should have a modular design to allow an easy integration of future sensors and effectors according to specific national needs and threat evolution;
- The system should be easy to integrate into the legacy and future platforms.

MWS subsystem

- The MWS should cover missile warning and hostile fire indicator;
- The MWS may combine various technologies, including electro-optic detection;
- The proposed MWS may incorporate additional capability;
- The MWS should offer different modes of operation.

RWR subsystem

- The RWR should have a high probability of interception;
- The RWR should be a fully digital receiver;
- The RWR should have a high accuracy and dynamic range of measurements;
- The RWR should have processing for classification/identification;
- The RWR should be modular for specific national programing;
- The RWR should be low cost.

CMDS subsystem

- The CMDS should be modular for specific national programming.

EAD subsystem

- The EAD should be self-powered;
- The EAD should be self-programmed at the ejection;
- The EAD should have self-detection and processing channels;
- The EAD should be effective against modern threats guided through electromagnetic spectrum;
- The EAD should be modular for specific national programming.

DIRCM subsystem

- The DIRCM should cover a high range of signatures;
- The DIRCM should be compatible with the MWS above;
- The DIRCM should be compatible with all threats;
- The DIRCM should have a low drag turret;
- The DIRCM should be easy to install and maintain;
- The DIRCM should be based on European technology;
- The DIRCM should allow multiband operation;
- The DIRCM should be low cost compared to current systems.

Hard-kill solutions

- Proposed solutions should be compatible with a wide range of platforms;
- Proposed solutions should have large space coverage;
- Proposed solutions should take into account security aspects and compatibility with the Rules of Engagement (RoE);
- Proposed solutions should be low cost.

EW manager subsystem

- The EW manager should be an advanced smart subsystem able to autonomously coordinate sensors and effectors from one or several platforms and effectively support the crew in the decision making process in operational conditions;
- The EW manager should manage, control and operate sensors and countermeasures in various mission states and modes, including combined actions;
- The EW manager should provide the “situation awareness”;
- The EW manager should generate warnings in presence of predefined dangerous threats;
- The EW manager should support Man-Machine Interface (MMI) by providing data to be presented on the on-board display;
- The EW manager should provide data to be sent to external platforms or bases (through tactical data link);
- The EW manager should monitor EW suite status (BITE[65] function);
- The EW manager should manage EW data and signal recording for post analysis.

[65] Built-in test equipment.

Expected impact

With reference to currently available self-protection systems:

- Increased coverage in term of threats' types;
- Ability to tackle new-generation threats;
- Ensure European autonomy in the survivability domain;
- Versatility to cover a wide range of platforms and save costs in integration/installation and specific development through modular design.

1.9.3. Topic EDIDP-ACC-3MACS-2020 – EU multiplatform mission management capabilities for air combat systems

The development of a consolidated EU perspective with regard to mid- and long term applications, requirements, solution concepts and technology needs for a EU multiplatform mission management capability for air combat. This call intends to provide a consolidated baseline within the EU Member States and industry in this subject matter, to identify potential "quick-wins" for European air combat capabilities and to set the starting point to ensure a high level of interoperability amongst future developments and products in this domain to finally support the path of achieving the desired air superiority.

Specific challenge

Driven by the anticipated future threats in the air combat domain, mainly the existence and proliferation of highly integrated and networked air defence systems, fighter aircrafts of fifth generation and the expected limitations in use of the electromagnetic spectrum, the Capability Development Plan (CDP) highlights the need to integrate and "combine manned and unmanned platforms in a larger operational system".

The development of future air combat systems will be characterized by an information centric networked approach. The next generation of air combat capabilities is envisaged as a combination of manned platforms – both newly developed and enhanced legacy fighter aircraft platforms–, teamed with a variety of unmanned systems, all equipped with a diversity of sensors and/or effectors.

To enable the variety of different assets to operate during an air operation together jointly and synchronized, to share sensor and effector resources, to share information and situational awareness overall leading to information and ultimately decision superiority to achieve the mission, a highly integrated multiplatform mission management capability will be required.

In the context of this call, this multiplatform mission management capability must be understood as the capability to enable a group, composed of several air combat platforms (manned and unmanned) of different types and capabilities, achieving a common mission task or goal. Moreover, such multiplatform mission management capability must be able to coordinate several groups of air combat platforms in time and space.

Current European air combat systems (*e.g.* Rafale, Eurofighter, Gripen, European MALE RPAS) are foreseen to be embedded as "enhanced legacy platforms" in the future air combat system(s). Concepts for other unmanned air combat platforms (*e.g.* remote carriers, smart cruise missiles, UCAV[66]) are under development in several EU Member States. In the context of multiplatform command and control/mission management, concepts and demonstrators (such as manned-unmanned teaming) are also in development.

With regard to integration and combination of air combat platforms in Europe, on the long-term within a future air combat system, on the mid-term by trying to enhance European air

[66] Unmanned combat aerial vehicle.

combat capabilities by partial combination and integration of existing systems, the challenges are:

- EU Member States lack a consolidated perspective of use cases, applications, high level operational and technical requirements with regard to multiplatform management capabilities between air combat platforms, manned and unmanned;
- the further development of platform and operating concepts and architectures in national EU Member State silos is prone to hamper interoperability of later on systems and products, causing the need for further investments to harmonize developments at a later stage;
- the need for a contemporary initiation of the development of early multiplatform mission management capabilities based on legacy fighter aircraft platforms to enhance European air combat capabilities in the mid-term, by ensuring later on interoperability with future air combat systems.

Scope

The proposals must address the generation of a consolidated perspective of interested EU Member States and industries with regard to mid- and long-term development of an EU multiplatform management capability for air combat systems, manned and unmanned.

The proposals must consider manned fighter aircraft from EU origin (and potentially connectivity with those from non-EU origin), and unmanned combat platform assets/concepts like "Remote Carriers", UCAVs and "Smart Cruise Missiles".

The proposals must consider scenarios for air combat operations in contested and highly contested environments.

Targeted activities

The proposals must cover the study and design, not excluding downstream activities, of an EU multiplatform management capability for manned and unmanned air combat systems.

The targeted activities must in particular include:

- the development of potential use cases, scenarios and applications for multiplatform mission management capabilities;
- the derivation of high level operational and technical requirements including human factors or artificial intelligence (AI) elements with regard to multiplatform mission management capabilities;
- the description of the solutions' space by selected multiplatform mission management concepts;
- the assessment of EU existing technologies with regard to multiplatform mission management and respective technological enablers (*e.g.* network connectivity);
- a gap analysis of technologies to define respective roadmaps and conduct cost risk mitigation evaluation;
- the identification of "first" mid-term multiplatform mission management application (*i.e.* potential "quick-wins" based on "enhanced legacy fighter aircrafts");

- the study, design and implementation of one or several small scale demonstrator(s) and its (their) concept assessment. The output must include:
  - a dynamic display of selected contemporary technologies and small-scale technological demonstrators, in order to make tacit expert knowledge accessible and conduct a nation-specific exchange;
  - the assessment of operational, technical and legal boundaries and limitations, and national specifics.

As a *modus operandi*, the proposed action must ensure the participation of respective ministries of defence' representatives, including through interviews and workshops.

Main high-level requirements

The proposed capability should at least be based on:

- significantly improving mission capability and mission efficiency;
- existing and emerging flight safety and airworthiness rules;
- mission joint operativity within a fleet of mixed air platforms;
- MUM-T key operational aspects (including joint ISTAR[67] supporting combat);
- service oriented architecture principles;
- connectivity/interoperability management principles to set up secure, resilient, agile communication infrastructure and architecture and to provide connectivity services;
- data distribution management principles;
- existing and to be defined open standards and other European initiatives (*e.g.* ECOA[68], ESSOR[69]).

The implemented capabilities should provide enhanced cyber secured interoperability of Member States' systems involved in air operations (including C2 ground or air assets) and be upgradeable and scalable.

The proposed capability should ensure interoperability with NATO and consider other coalition situations.

Expected impact

- Generation of a consolidated EU perspective of the subject matter within EU Member States' ministries of defence and EU industry;
- Identification of potential "quick-wins" in the context of multiplatform mission management applications with regard to mid-term enhancements of European air combat capabilities;
- Generation of prerequisites and inputs for the long-term development of future air combat systems definition;
- Provision of a vehicle for cross-ministries of defence and cross-industry exchange in the subject of multiplatform mission management;

[67] Intelligence, Surveillance, Target Acquisition & Reconnaissance.

[68] European Component Oriented Architecture.

[69] European Secure Software defined Radio.

- Provision of a potential starting point for developing EU standards to enable further development of interoperable products by EU nations and industry;
- Evaluation of increased mission capability, efficiency and force in air combat missions;
- Identification of technologies for the mission management capability for enhancement of EU Member States combat capability;
- Generation of European technology for multi mission management independent of third countries.

1.10. Call EDIDP-SVTE-2020 – Simulation and virtualisation tools and equipment for training, exercises, systems design, development and integration, testing and validation

Virtual reality and distributed synthetic environments are increasingly important to better train armed forces for real-life operations, including requirements for command structures operations from the tactical to the strategic level, tools for decision-making and civilian-defence cooperation and CBRN training, manned-unmanned teaming, but also to be used for systems design, development and integration.

Proposals are invited against the following topic

EDIDP-SVTE-2020: Modelling, simulation and virtualisation tools and equipment for training, exercises, systems design, development and integration, as well as testing and validation.

Budget

The Union is considering a contribution of up to EUR 3 500 000 to support proposals addressing the above-mentioned topic and its associated specific challenge, scope, targeted activities and main high-level requirements.

Specific challenge

The Global Strategy for the European Union's Foreign and Security Policy defines an integrated approach to conflicts "at all stages of the conflict cycle, acting promptly on prevention, responding responsibly and decisively to crises, investing in stabilization and avoiding premature disengagement when a new crisis erupts".

The current European simulation structure (in the sense of simulators and their interconnection) and European simulation and wargaming capabilities are fractured into many national systems and infrastructures with a limited interoperability and a lack of common understanding and definition of simulation models employed.

Scope

The proposals must address the development of a distributed simulation infrastructure including basic simulation data allowing cooperative simulation between Member States, their military and civil organisations, as well as non-state actors originating from Member States.

The proposals must encompass the strategic level down to the tactical level and scenarios from the high intensity conflict to peace enforcement, stabilisation, counter-insurgency and anti-terrorism operations. Furthermore, civil-military cooperation (CIMIC) for the above-mentioned scenarios, protection of critical infrastructure and disaster relief must be included.

The proposals must in particular support the following applications:

- Simulation-based training and exercising for military and civilian staffs:

  - Preparation training for EU-Battlegroups for CSDP (Common Security and Defence Policy) missions;
  - Training on disaster relief scenarios;
  - Support to the integration of RPAS and drones in the national air-space (RPAS[70]-ATI[71]);
  - Employment of artificial intelligence (AI) for simulated military/civilian force behaviour to reduce staffing of simulation.
- Preparation of force deployment:
  - Validation of EU force deployment plans;
  - Employment of decision support tools for evaluation of scenarios.
- Concept development and evaluation:
  - Identification and quantification of deficiencies;
  - Simulative evaluation of new equipment and systems;
  - Definition and evaluation of new organisations, tactics and procedures;
  - Support of projects, preferably corporately developed by EU Member States;
  - Employment of data mining and operations research tools.

The proposals must address scenarios in either one or multiple military domains (land, sea, air, space, cyber).

Targeted activities

The proposals must cover study, design and prototyping of a solution, not excluding downstream activities.

The targeted activities must in particular include:

- preliminary/feasibility studies:
  - analysis of EU Member States' defence national standards and regulations concerning simulation;
  - analysis of NATO standards and regulations concerning connection of simulations;
  - analysis of civilian communication and data exchange standards;
  - analysis of commonality of requirements;
  - definition of requirements;
  - definition of CONOPS (Concept of Operations).
- design:
  - definition of the system architecture (hardware, software, networks);
  - definition of the security environment;
  - proposal for a test-case as a basis for the demonstrator;
  - definition of an effects database.
- prototyping - demonstrator implementation:
  - integration of a system demonstrator for risk mitigation;
  - presentation of study results and execution of a demonstration with a test scenario.

[70] Remotely piloted air system.

[71] Air traffic integration.

A detailed planning of the potential subsequent project phases must be generated, including the identification of implementation priorities, according to the operational needs of the EU and its Member States.

Main high-level requirements

The system must fulfil the following main high-level requirements:

- state-of-the-art system, with modern, intuitive user interfaces supporting operators in all their operational, technical and training needs. Usability must be the cornerstone of the system design allowing the rapid installation, administration, operation and training;
- selection of technological solutions with a strong focus on obsolescence management;
- the system architecture must be designed in accordance with the modularity principle in order to deliver simulation services to future operational capabilities and to interface with multiple sources, allowing EU defence projects to be linked or implemented through this one;
- the proposed architecture must be based on a modern service-oriented architecture with an extensive use of open standards, allowing full compatibility with NATO and national systems, both military and civilian. Specifically the system must be interoperable with a federated simulation network;
- effective use of communications, covering also tactical levels. The architecture must operate in a full IP communication network that must be able to integrate different transmission mechanisms (WAN[72] segments, SATCOM[73], DIS[74], HLA[75], *etc*.). It must be able to seamlessly use the available transmission mechanisms and adapt the information flows to their specific characteristics;
- the architecture must be able to work simultaneously in different security domains and handle the information security requirements to properly control the information flows between these domains as well as external systems. A security domain must be able to address the community of a project only and offer adequate security requirement securing the confidentiality of the information of the project;
- the architecture must be dynamic, scalable and resilient, capable of easily integrating all the actors and nodes for each simulation scenario or application;
- the architecture must be able to be deployed over distributed simulation centres. The system must be deployable over COTS[76] IT equipment and must be able to operate in virtualized environments in conjunction with specific security equipment, such as Information Exchange Gateways (IEGs), Firewalls, Intrusion Detection and Prevention Systems (IDSs and IPSs), *etc*. The feasibility of an architecture based on cloud concepts (either private or hybrid) must specifically be analysed;
- the architecture must be able to support specified availability requirements providing an open, scalable, high availability and transparent failover architecture;
- 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;

[72] Wide area network.
[73] Satellite communications.
[74] Distributed interactive simulation.
[75] High level architecture.
[76] Commercial of the shelf.

- the architecture must be adapted to the doctrine generated in Europe.

The architecture of the distributed simulation system must take into consideration all necessary future elements, and in particular:

- simulation and communication equipment and infrastructure, in order to be able to exchange information between the Member States' simulation centres and information systems. This may require the use of dedicated terrestrial networks and satellite links, hub infrastructure and terminals;
- the infrastructure to setup dedicated simulation centres, including facilities for operators, data centres, and all the associated equipment (such as operators' equipment, voice / video communications, local communications, *etc.*);
- deployable simulation centres, providing operators with workstations, a deployable data centre, communication means and the required infrastructure;
- architecture designed for security accreditation and cyber defence in order to prevent cyber-attacks and to protect the information.

Expected impact

- Develop critical enablers for CSDP operations and EU Battlegroup missions;
- Reduce the minimum reaction time for deployment of European military missions;
- Integrate simulation means provided by Member States, EU forces, NATO and civil agencies;
- Improve situational awareness, resilience and security of EU operations;
- Create a reference simulation architecture that will improve the capabilities of the European defence industry to develop and supply state-of-the-art simulation systems;
- Reinforce interoperability of EU Member States’ armed forces;
- Reduce the cost of European military missions;
- Reduce training and travelling costs thanks to distributed simulation.

1.11. Call EDIDP-AI-2020 – Defence technologies supported by artificial intelligence

Artificial Intelligence (AI) is expected to help overcoming the “3V challenge” (volume, variety and velocity) of big data[77] while providing data processing that includes a controlled level of decision based on AI’s knowledge.

This call aims at defining cutting-edge technologies and software solutions to improve the current situation in the following two functional areas:

1. Situational awareness and decision-making support (*e.g.* common recognised picture in different domains: land, sea, air, space or cyber).

2. Planning (*e.g.* logistic planning, operational planning), including modelling and simulation.

These solutions notably include tools that can help operators in their understanding of an operational situation, enabling:

- their decision-making process (task 1);
- the optimization of the use of their assets (task 2).

For practical reasons relating to a multi-national project involving multiple industry partners, and taking into account the novelty of this topic, the data used to support the activities under this call must be unclassified and open.

Proposals are invited against the following topic
EDIDP-AI-2020: Defence capabilities supported by artificial intelligence.

Budget
The Union is considering a contribution of up to EUR 5 700 000 to support proposals addressing the above-mentioned topic and its associated specific challenge, scope, targeted activities and main high-level requirements.

Specific challenge
Modern forces rely on various systems and platforms (*e.g.* satellites, aircrafts, UAVs[78], ships, ground vehicles) that generate massive data (*i.e.* big data) from different sensor/effector types and timeframes (*e.g.* real-time fluxes, weekly data reports, reactive acquisition missions). In addition, specific domains[79] may also collate open data to flesh out mobiles identification.

The growing amount of data may offer the opportunity of a more efficient use of assets provided that processing tools, customized for existing communication links, are able to extract relevant information from data sources.

[77] The data storage architecture is not part of this call, even though it is recognized that it may have a significant impact on data processing using AI techniques.
[78] Unmanned air vehicles.
[79] Such as maritime surveillance.

This call aims at helping the operator to leverage multi-source intelligence (multi-INT) data in large collections of data.

AI techniques should be looked upon with attention, as it may offer a significant potential to provide solutions maximizing performance at minimal cost. It is required to select different AI techniques most suited to the behaviour of the process being optimized.

Traceability and responsibility have also to be addressed properly within a supervised approach and black boxes components have to be minimized. Furthermore, vulnerabilities and potential failures have to be dealt with.

Scope

The proposals must address or contain description of:

- functional analysis of typical scenarios covering both areas:
  - situational awareness and decision making support;
  - planning.
- fieldable concept that enables the use/implementation of AI techniques, among which, but not limited to, machine learning and neural networks, mixed with other typical AI paradigms (inferential engines, fuzzy logic);
- algorithm prototyping, implementation and verification, including the data sets and metrics to be used to do so;
- tools development including algorithm insertion and demonstration (PoC[80]);
- concepts[81] of AI-based applications' store for end-users.

Targeted activities

The proposals must cover the study, design, prototyping and testing of the AI-based technologies and solutions (*e.g.* System of systems/Subsystem of systems PoC).

These activities must in particular include:

- identification of feasible use cases and related requirements definition for AI-based application contexts;
- scouting of contemporary technology that can support agile design and implementation activities;
- collection of data representative of the use cases;
- implementation of verification metrics (scenario simulation using the collected data);
- implementation of technology demonstrator(s);
- verification of the technology demonstrator(s) through simulation of scenarios.

Main high-level requirements

Tools associated to the different scenarios (use cases) should be developed:

[80] Proof of concept.

[81] *e.g.* Cloud architecture in platform as a service (PaaS) mode.

- addressing properly traceability and responsibility in the design and development activities;
- giving clear view of cyber vulnerabilities and potential failures.

The following requirements should be fulfilled:

<u>For task 1 relating to situational understanding and pictures</u>

- The operator should be assisted by the tool through both precise information that it has inferred from data and high-level representations, in order to facilitate quick grasp of the situation;
- The tool should be multi-INT in that it infers the best possible information from all possible sources, including but not limited to:
  - non sensitive ISR data from a wide variety of sensors/vectors;
  - current and past mission data;
  - history of events and operator decisions;
  - open-source data from structured databases as well as unstructured in-the-wild data (*e.g.* social networks).
- The tool should be agnostic to specific sources of data;
- The tool should propose acquisition missions with existing means, whenever it judges it provides the best complement of information;
- The tool should be non-exclusive, in the sense that lack of some of the usual sources does not prevent information inference (only degrades it);
- The tool should provide short-term information, such as current interest events as well as predicted situations (*e.g.* locations and dates of predictable events).

<u>For task 2 relating to mean-of-effect optimization</u>

- The operator should be assisted by the tool in selecting an effector or a combination of effectors thereof to best handle the mission at hand;
- The tool should be able to provide lists of possible solutions to mission events occurrence for operator choice and consider returning feedback to improve tool's knowledge base;
- The tool can require some manual filling of effector characteristics, but should infer, at minimal performance drop, the missing parameters (based on similarity with other systems, for instance).

For all of these contexts of use, it is important to have "trustable" or "explainable" tools. This means for AI-based capabilities to minimize as far as possible the use of black boxes, which should only be allowed for low level components or to perform extensive testing of those black boxes (*e.g.* in case of machine learning). This allows having the decision making rationale, as well as offering evolution traceability, at capability level.

<u>**Expected impact**</u>

- Presence in the system of innovative techniques that support the operators in some of their most critical functions, offload them (relief from manual operations), thereby maintaining their analytical ability to operate as supervisors;

- Mark the difference between commercial use of the AI and military use of the AI (*inter alia*: attention to traceability and responsibility);
- Improvement of the reaction time for mission deployment by AI-supported decision-making;
- Cost and availability gains by optimizing the means-of-effect;
- Increase of the overall system performance as new technologies will give better results in terms of total defence effectiveness;
- Enabler for rapid integration of multiple data sources to support field and based personnel using deployable machine learning and AI models;
- A validation approach that ensures the correct use of AI models in mission critical contexts;
- A set of standards’ proposals that allows multi-national collaboration and sharing of machine learning models for military use;
- Big data management and congruent pattern identification;
- Increase the European technological sovereignty in the field of AI for defence applications.

1.12. Call EDIDP-SME-2020 – Innovative and future-oriented defence solutions

The development of innovative and future-oriented defence products and technologies relies on the innovation capacity of Small and Medium-sized Enterprises (SMEs). This call for proposals targets innovative defence products, solutions and technologies and is devoted to SMEs.

Proposals are invited against the following topic

EDIDP-SME-2020: Innovative defence products, solutions, materials and technologies, including those that can create a disruptive effect and improve readiness, deployability, reliability, safety and sustainability of EU forces in all spectrum of tasks and missions, for example in terms of operations, equipment, infrastructure, basing, energy solutions, new surveillance systems.

Budget

The Union is considering a contribution of up to EUR 10 000 000 to support several proposals addressing any subject of interest for defence, while considering a contribution of up to EUR 2 500 000 to support an individual proposal.

Several actions, addressing different defence products, solutions, materials and technologies, may be funded under this call.

Specific challenge

This category encourages the driving role of SMEs in bringing forward innovation, agility and ability to adapt technologies from civil to defence applications, to turn technology and research results into products in a fast and cost-efficient way.

Scope

The proposals must address innovative defence products, solutions and technologies, including those that can create a disruptive effect and improve readiness, deployability and sustainability of EU forces in all spectrum of tasks and missions, for example in terms of operations, equipment, basing, energy solutions, new surveillance systems.

The proposals could address any subject of interest for defence, such as, but not limited to, the following:

- Cybersecurity solutions for the protection of the future security and defence systems (*e.g.* command and control, logistics, embedded systems, distributed simulation);
- Future compounds/smart basing technologies development;
- Development of innovative methods or methodologies for comprehensive technical requirements setting such as concurrent design;
- Future Mine Counter Measures (MCM) capabilities operating autonomous underwater systems, coping with current capability gaps in securing Sea Lines of Communication;
- Integrated maritime surveillance system, combining legacy assets with new, innovative solutions;

- Portable bacteriological and chemical future detection systems;
- Future soldier CBRN (Chemical, Biological, Radiological and Nuclear) protection equipment and integration;
- Innovative intelligence tools for early warning and countermeasure deployment support to counter CBRN threats;
- Wearable orthosis equipment and exoskeletons to increase strength capabilities and minimize stress of future soldiers;
- Autonomous and remote-controlled unmanned systems for safe medical evacuation of injured soldiers during military operations;
- End-to-end solutions for artificial intelligence in defence & security key strategic issues;
- Command and control systems designated for individual soldier-squad up to brigade Command, post logistic information system for maintenance, transport, medical, management;
- Armoured medium and light vehicle;
- Tactical logistic trucks;
- Protected, cooled and connected shelter solutions for fixed and mobile command post for EU operations;
- Future effective and collective CBRN protection capacity to civil population, military and their equipment;
- Mobility support deployable solution for amphibious and airmobile (helicopter) operations;
- Innovative battery for future infantry portable system (radio set, optronic, *etc.*) and for weapon system (missile) ignition;
- Innovative solutions (bio-based) for fuel production from organic waste to support military operations and energy self-sufficiency in remote areas;
- Innovative passive systems (solar-tracking) systems for energy production based on renewable sources to support military operations in remote areas;
- Innovative software systems for processing of aerial images and videos through hyperspectral imaging (for metadata/telemetry information extraction and exploitation in C2 systems);
- Integrated management system for assets and services required in emergency situations in the framework of EU defence operations, in order to increase sustainability of EU forces;
- Nanomodified composite materials and related production processes and design procedures for reinforcement of existing armours of military vehicles including bonding test equipment;
- Development of a minefields mapping system using unmanned aircraft;
- High capacity communications for UAVs (Unmanned Air Vehicles) in beyond line-of-sight applications;
- Medical virtual reality training simulator;
- Unmanned semi-fixed sea platforms;
- Additive manufacturing enhancing the logistic performance by provide to military end-users possibilities to produce spare parts using additive manufacturing solutions, particularly in the context of overseas operations, including manufacturing methods, diagnostic equipment, surface treatment, residual stress modelling and analysing, cracks formation or chemical corrosion in metals and multimaterials bonds or connection;

- Development of a capability to collect and process operational and oceanographic data, in particular those coming from gliders;
- Development of counter-UAS (Unmanned Air System) capability based on mini-UAS swarms;
- Secure high capacity communications for UAVs in beyond line-of-sight applications;
- Augmented-reality combat helmet featuring night-vision and ally or enemy position display, including artificial intelligence functionalities;
- Intelligent, dynamic and robust control of the quality of service in hybrid satellite-terrestrial telecommunication networks;
- Enhancing maintenance, repair and operating equipment including metal improving techniques, non-destructive diagnostic methods for fixed wing or rotary wing aircrafts;
- Innovative composite materials and transparent displays for existing and next generation military armoured vehicles;
- Development of an innovative set of deployable, unattended and remotely controlled network of sensors for ISTAR[82] mission on the battlefield;
- Hydropneumatics rotary suspension technology for high mobility tracked armoured vehicles;
- Camp 4.0 infrastructure, based on real time cloud and on-premise digital twin benefiting from blockchain technologies' robustness, able to channel all currently optimized logistics needs, such as chain of spare parts, maintenance, energy consumables;
- Solutions based on artificial intelligence for standardization of the automatic steering and manoeuvring systems of vessels in a cost-effective manner;
- Photonics-based SIGINT[83] payload for class II RPAS[84];
- Easy-to-handle low-tech diagnostic kits for selected chemical and biological threat agents, providing sensitive and low false positive response to detect exposure to classes of chemical and biological threat agents;
- Innovative future-oriented communication capabilities such as, but not limited to, quantum communications or high-speed secure free space optical communication.

Targeted activities

The proposals must cover any single activity or combination of activities listed in Article 6(1) of the EDIDP regulation:

- Studies;
- Design;
- System prototyping;
- Testing;
- Qualification;
- Certification;
- Development of technologies or assets increasing efficiency across the life cycle of defence products and technologies.

[82] Intelligence, surveillance, target acquisition and reconnaissance.
[83] Signal intelligence.
[84] Remotely piloted aircraft systems.

Given the importance of time-to-market for SMEs, the proposals are expected to cover more than only studies or design.

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;
- Building innovation capacity across Europe by involvement of SMEs that can make a difference in the future;
- Potential for future market creation for SMEs.

3. Conditions for the calls

The following section provides all the necessary conditions to submit proposals in response to the calls described in section 2.

3.1. Opening dates, final date for submission and indicative budgets

Calls	Topics	Budgets in EUR (2020)	Opening date[85]	Final date for submission[86]
EDIDP-CBRN-2020	EDIDP-CBRN-DEWS-2020	Up to 13 500 000	15 April 2020	1 December 2020
	EDIDP-CBRN-MCM-2020			
EDIDP-UCCRS-2020	EDIDP-UCCRS-MCM-2020	Up to 22 500 000	15 April 2020	1 December 2020
	EDIDP-UCCRS-MUAS-2020			
	EDIDP-UCCRS-EDD-2020			
EDIDP-CUAS-2020	EDIDP-CUAS-2020	Up to 13 500 000	15 April 2020	1 December 2020
EDIDP-CSAMN-2020	EDIDP-CSAMN-SDN-2020	Up to 14 300 000	15 April 2020	1 December 2020
	EDIDP-CSAMN-EDICT-2020			
EDIDP-SSAEW-2020	EDIDP-SSAEW-SC2-2020	Up to 22 500 000	15 April 2020	1 December 2020
	EDIDP-SSAEW-SSAS-2020			
	EDIDP-SSAEW-EW-2020			
EDIDP-MSC-2020	EDIDP-MSC-IS-2020	Up to 20 000 000	15 April 2020	1 December 2020
	EDIDP-MSC-MFC-2020			
	EDIDP-MSC-CRPS-2020			
	EDIDP-MSC-NS-2020			
EDIDP-NGPSC-2020	EDIDP-NGPSC-LRIF-2020	Up to 7 000 000	15 April 2020	1 December 2020
	EDIDP-NGPSC-PGA-2020			
EDIDP-GCC-2020	EDIDP-GCC-2020	Up to 9 000 000	15 April 2020	1 December 2020

[85] The authorising officer by delegation responsible for the call may decide to open the call up to one month after the envisaged opening date.

[86] All deadlines are at 17:00:00 Brussels local time. The authorising officer by delegation responsible for the call may delay the final date for submission subject to the evolution of the coronavirus crisis. Please check regularly the Funding and Tender portal for update.

Calls	Topics	Budgets in EUR (2020)	Opening date[87]	Final date for submission[88]
EDIDP-ACC-2020	EDIDP-ACC-CH-2020 EDIDP-ACC-SPS-2020 EDIDP-ACC-3MACS-2020	Up to 22 000 000	15 April 2020	1 December 2020
EDIDP-SVTE-2020	EDIDP-SVTE-2020	Up to 3 500 000	15 April 2020	1 December 2020
EDIDP-AI-2020	EDIDP-AI-2020	Up to 5 700 000	15 April 2020	1 December 2020
EDIDP-SME-2020	EDIDP-SME-2020	Up to 10 000 000	15 April 2020	1 December 2020

[87] The authorising officer by delegation responsible for the call may decide to open the call up to one month after the envisaged opening date.

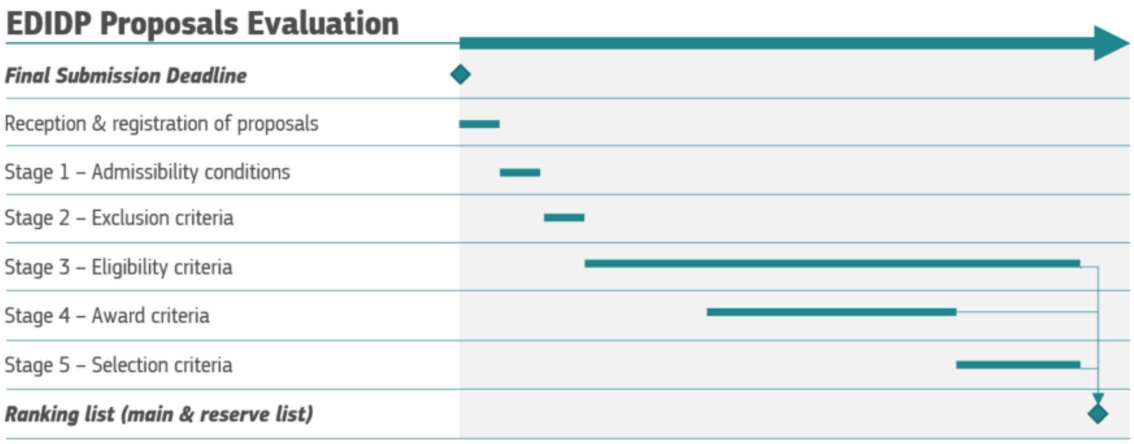
[88] All deadlines are at 17:00:00 Brussels local time. The authorising officer by delegation responsible for the call may delay the final date for submission subject to the evolution of the coronavirus crisis. Please check regularly the Funding and Tender portal for update.

3.2. Evaluation procedure and conditions

The received proposals will be evaluated by the Commission on the basis of the procedure and conditions described below.

3.2.1. Procedure

The evaluation of the proposals will be performed by the Commission following a multi-stage procedure:

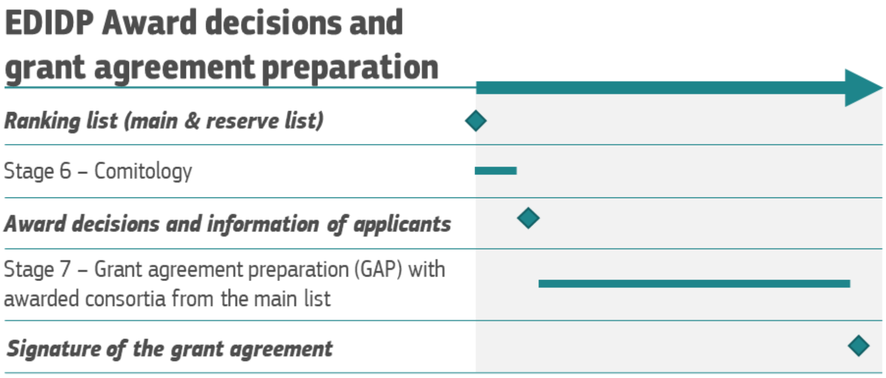


- Stage 1 will consist in determining if the received proposals meet the admissibility conditions (see 3.2.3). Proposals failing to meet admissibility conditions will be rejected.
- Stage 2 will consist in determining if the admissible proposals fall under exclusion grounds (see 3.2.4). Proposals which fall under exclusion grounds will be rejected.
- Stage 3 will consist in assessing the proposals against eligibility criteria (see 3.2.5):
  - Eligibility of the proposed action;
  - Eligibility of the entities involved in the action.

  Proposals which fail to meet any of the eligibility criteria will be rejected. The assessment of the eligibility will extend until all conditions are assessed, possibly after the evaluation of the award criteria with the assistance of external experts. Considering the principle of proportionality and the complexity of some criteria, the Commission will complete the eligibility assessment exclusively for proposals above the threshold for the award criteria.
- Stage 4, for which the Commission will be assisted by independent experts, will consist in the assessment of the proposals against the award criteria, resulting in a scoring of the proposals (see 3.2.6).
- Stage 5 will consist in assessing the proposal against selection criteria (see 3.2.7):
  - Financial capacity of the applicants;
  - Operational capacity of the applicants.

  Proposals which fail to meet any of the selection criteria will be rejected.

Stages 1 to 5 will result in a ranking per call (main and reserve list).


EDIDP Award decisions and grant agreement preparation
Ranking list (main & reserve list)
Stage 6 – Comitology
Award decisions and information of applicants
Stage 7 – Grant agreement preparation (GAP) with awarded consortia from the main list
Signature of the grant agreement

- Stage 6: the ranking will be submitted to comitology for approval by the Programme Committee of Member States. The outcome will be the award decisions and the information of the successful and unsuccessful applicants.
- Stage 7 will consist in inviting coordinators of awarded consortia to start the grant agreement preparation (GAP): negotiation and signature of the grant agreement by or in the name and on behalf of the Commission.

3.2.2. Indicative timeline for evaluation and grant agreement signature

Information of the applicants on the outcome of the evaluation: maximum six months from the final date for submission.
Indicative date for the signing of grant agreements: maximum three months from the date of informing successful applicants.

3.2.3. Admissibility conditions

The proposals submitted following the call for proposals must fulfil the following admissibility conditions:

- Applicants must submit their proposal in one of the official languages of the Union (English language is encouraged), using the submission form template available here.
- The submission form must be duly completed. *Applicants may usefully refer to the guide for applicants (available here) to do so.*
- One proposal must only be submitted against one topic.
    - Where a call is covering several topics (EDIDP-CBRN-2020, EDIDP-UCCRS-2020, EDIDP-CSAMN-2020, EDIDP-SSAEW-2020, EDIDP-MSC-2020, EDIDP-NGPSC-2020 and EDIDP-ACC-2020), one proposal must only address one topic of this call.
    - Proposals in response to the call EDIDP-SME-2020 must address one clearly identified product, solution, material or technology which is of interest for defence. The provided list of subjects inside the call text is only indicative.

- All proposals must be provided in an electronic version in a searchable[89] pdf format (and where requested, excel format) on a USB stick or a CD-ROM. In addition to this electronic version, applicants are allowed to submit a paper copy. In case of discrepancies between the electronic and paper copies, the electronic copy will be the reference. In case of discrepancies between the pdf and excel files, the pdf file will be the reference.
- All proposals must be readable, accessible and printable.
- Proposals must be submitted before the final date for submission (evidence of timely delivery) specified in the table of section 3.1.
- Proposals must be submitted according to one of the following options:
  - Option a: **sent by registered mail** (date of postmark serving as evidence of timely delivery) to the following address:

    European Commission
    Directorate-General for Defence Industry and Space
    EDIDP Call 2020
    Unit A.3
    Office address: BREY 09/028
    B-1049 Brussels, Belgium

  - Option b: **sent by courier services** (date of deposit slip serving as evidence of timely delivery) to the same address as in option c.
  - Option c: **delivered by hand** (date of acknowledgement of receipt by the Commission serving as evidence of timely delivery) to the following address:

    European Commission
    Directorate-General for Defence Industry and Space
    EDIDP Call 2020
    Unit A.3
    Office address: BREY 09/028
    Service central de réception du courrier
    Avenue du Bourget, 1-3
    B-1140 Bruxelles, Belgique

Failure to comply with those conditions will lead to rejection of the proposal.

If the applicants deem necessary to include classified information in their proposal, they must contact the Commission at the following email address (EC-EDIDP-proposals@ec.europa.eu) well before the final date for submission of the call, in order to arrange the delivery of their proposal.

3.2.4. Exclusion grounds

The objective of the exclusion grounds is to specify the cases in which applicants must be excluded from participating in the call procedure or from being awarded a grant.

[89] Scan pdf is also accepted for signed supporting documents.

These situations are described in Article 136 of the Financial Regulation. They include bankruptcy, grave professional misconduct, non-compliance with social or tax obligations, involvement in a criminal organisation, money laundering or any other illegal activity.

Applicants must declare on their honour that they are not in one of the situations of exclusion referred to above. To this effect, declarations on honour must be included in the grant application to be signed by all applicants (see Annexe 3 to the submission form).

Depending on a risk assessment, the successful applicants may be requested to provide further evidence to demonstrate that they do not fall under the exclusion criteria.

However, the authorising officer responsible must waive the obligation for an applicant to submit evidence, when such evidence has already been submitted for the purposes of another grant or procurement procedure, provided that the documents are not more than one year old and the applicant confirms that they are still valid.

3.2.5. Eligibility criteria

Assessment against eligibility criteria will be performed based on evidence the applicants must provide at the time of the submission of their proposal (*see relevant section of the guide for applicants for example of expected evidence against each criterion*).

The eligibility criteria fall into two types:

- Eligibility criteria for the proposed action;
- Eligibility criteria for the entities involved in the action.

The eligibility criteria are listed below.

Proposals that will fail to meet any of these eligibility criteria will be rejected.

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 undertaking must inform the Commission, which must assess whether the eligibility criteria continue to be met and must address the potential impact on the funding of the action.

➢ **Eligibility criteria for the proposed action**

- The action must address the development phase of new defence products and technologies and/or the upgrade of existing products and technologies;
- Where addressing upgrade, the use of pre-existing information needed to carry out the action must not be subject to a restriction by a third country or by a third-country entity, directly, or indirectly through one or more intermediary undertakings;
- The action must only address one or more of the following activities:

  (a) studies, such as feasibility studies, and other accompanying measures;

  (b) the design of a defence product, tangible or intangible component or technology as well as the technical specifications on which such design has been developed, including partial tests for risk reduction in an industrial or representative environment;

(c) the system prototyping of a defence product, tangible or intangible component or technology;
(d) the testing of a defence product, tangible or intangible component or technology;
(e) the qualification of a defence product, tangible or intangible component or technology;
(f) the certification of a defence product, tangible or intangible component or technology;
(g) the development of technologies or assets increasing efficiency across the life cycle of defence products and technologies.

- The action must be carried out by undertakings cooperating within a consortium of at least three eligible entities which are established in at least three different Member States.
- At least three of those eligible entities established in at least two different Member States must not be controlled, directly or indirectly, by the same entity or must not control each other.
- The above-mentioned consortium must offer proof of viability by demonstrating that the costs of the action that are not covered by Union support are to be covered by other means of financing, such as by Member States' contributions.
- With regard to actions addressing activities (c), (d), (e), (f) or (g), the consortium must provide proof of their contribution to the competitiveness of the European defence industry by demonstrating that at least two Member States intend to procure the final product or to use the technology in a coordinated way, including through joint procurement where applicable.
- Actions addressing activity (b) must be based on common requirements jointly agreed by at least two Member States. If such actions address also activity (a) in the purpose to define such common requirements, these latter must be submitted at the latest following the completion of the activity (a), provided that it is demonstrated at the time of the submission of the proposal that at least two Member States intend to jointly agree on such common requirements.
- Actions addressing activities (c), (d), (e), (f) or (g), must be based on common technical specifications jointly agreed by the Member States that are to co-finance or that intend to jointly procure the final product or to jointly use the technology, as referred above, thereby strengthening the standardisation and interoperability of systems. If such actions address also activity (b) in the purpose to define such common technical specifications, these latter must be submitted at the latest following the completion of the activity (b), provided that it is demonstrated at the time of the submission of the proposal that at least two Member States intend to jointly agree on such common technical specifications.
- Actions for the development of products and technologies the use, development or production of which is prohibited by international law must not be eligible for funding.
- The results of actions which receive funding under the Programme must not be subject to control or restriction by a third country or by a third-country entity, directly, or indirectly

through one or more intermediate undertakings, including in terms of technology transfer.

In addition, a proposal will only be considered eligible if the proposed action addresses the scope and covers the targeted activities as described (in section 2 of this document) in the topic against which the proposal is submitted.

- **Eligibility criteria for the entities involved in the action**

In this sub-section, 'subcontractors involved in the action' refers to subcontractors with a direct contractual relationship to a beneficiary, other subcontractors to which at least 10 % of the total eligible cost of the action is allocated, as well as subcontractors which may require access to classified information in order to carry out the contract.

- Beneficiaries and subcontractors involved in the action must be public or private undertakings established in the Union.
- The infrastructure, facilities, assets and resources of the beneficiaries and subcontractors involved in the action which are used for the purposes of the actions funded under the Programme must be located on the territory of the Union for the entire duration of the action, and their executive management structures must be established in the Union.
- Where no competitive substitutes are readily available in the Union, beneficiaries and subcontractors involved in the action may use their assets, infrastructure, facilities and resources located or held outside the territory of Member States provided that that usage does not contravene the security and defence interests of the Union and its Member States, is consistent with the objectives of EDIDP (Article 3 of the EDIDP Regulation) and the provisions on ownership and intellectual property rights (Article 12 of the EDIDP Regulation). **The costs related to those activities will not be eligible for funding under the Programme.**
- For the purposes of the actions funded, the beneficiaries and subcontractors involved in the action must not be subject to control by a third country or by a third-country entity.
  - By derogation from this condition, an undertaking established in the Union and controlled by a third country or by a third-country entity must be eligible as a beneficiary or subcontractor involved in the action only if guarantees approved by the Member State in which it is established in accordance with its national procedures are made available to the Commission. Those guarantees may refer to the undertaking's executive management structure established in the Union. If deemed to be appropriate by the Member State in which the undertaking is established, those guarantees may also refer to specific governmental rights in the control over the undertaking. The guarantees must provide the assurances that the involvement in an action of such an undertaking would not contravene the security and defence interests of the Union and its Member States, as established in the framework of the Common Foreign and Security Policy pursuant to Title V of the TEU, or the objectives set out in Article 3 of the EDIDP Regulation. The guarantees must also comply with the provisions on ownership and intellectual property rights (Article 12 of the EDIDP

Regulation). The guarantees must in particular substantiate that, for the purpose of the action, measures are in place to ensure that:

- control over the undertaking is not exercised in a manner that restrains or restricts its ability to carry out the action and to deliver results, that imposes restrictions concerning its infrastructure, facilities, assets, resources, intellectual property or know-how needed for the purpose of the action, or that undermines its capabilities and standards necessary to carry out the action;
- access by a third country or by a third-country entity to sensitive information relating to the action is prevented and the employees or other persons involved in the action have national security clearances, where appropriate;
- ownership of the intellectual property arising from, and the results of, the action remain within the beneficiary during and after completion of the action, are not subject to control or restriction by a third country or by a third-country entity, and are not exported outside the Union nor is access to them from outside the Union granted without the approval of the Member State in which the undertaking is established and in accordance with the objectives set out in Article 3 of the EDIDP Regulation.

If deemed to be appropriate by the Member State in which the undertaking is established, additional guarantees may be provided.

- When carrying out an eligible action, beneficiaries and subcontractors involved in the action may also cooperate with undertakings established outside the territory of Member States or controlled by a third country or by a third-country entity, including by using the assets, infrastructure, facilities and resources of such undertakings, provided that this does not contravene the security and defence interests of the Union and its Member States. Such cooperation must be consistent with the objectives of EDIDP (Article 3 of the EDIDP Regulation) and must be fully in line with the provisions on ownership and intellectual property rights (Article 12 of the EDIDP Regulation). There must be no unauthorised access by a third country or other third-country entity to classified information relating to the carrying out of the action and potential negative effects over security of supply of inputs critical to the action must be avoided. **The costs related to those activities will not be eligible for funding under the Programme.**

For UK applicants: *Please be aware that following the entry into force of the EU-UK Withdrawal Agreement* on 1 February 2020 and in particular Articles 127(6), 137 and 138, the references to legal persons or undertakings established in a Member State of the European Union are to be understood as including legal persons or undertakings established in the United Kingdom. UK applicants, linked third parties and subcontractors involved in the action are therefore eligible to participate in EDIDP calls unless the Commission notifies the United Kingdom otherwise pursuant to Article 127(7)(b) of the Withdrawal Agreement. Applicants are strongly advised to regularly* *check EDIDP calls on the Funding & Tenders Portal for any updates concerning eligibility of UK applicants, linked third parties and subcontractors.*

** Agreement on the withdrawal of the United Kingdom of Great Britain and Northern Ireland from the European Union and the European Atomic Energy Community (OJ L 29, 31.1.2020, p. 7).*

3.2.6. Award criteria and scoring

Each proposal which complies with the admissibility, exclusion and eligibility conditions will be assessed and scored by the Commission, which will be assisted by at least three independent experts, against five (for actions covering only studies, design and/or life-cycle technologies) or six award criteria (for all other actions). The award criteria and the associated specific items that will be looked at are listed below and reflected in the submission form.

Scores will be attributed according to the principles:

- <u>for award criterion 1</u>: up to 5 points for subcriterion 1.1 and up to 5 points for subcriterion 1.2. The score for criterion 1 will be the average of the scores for subcriteria 1.1 and 1.2, each subcriterion having an equal weight of 1.
- <u>for award criteria 2 to 6</u>: up to 5 points for each award criterion.

Half-points will be allowed.

Scores will be attributed according to the following rationale:

0	The proposal fails to address the criterion or cannot be assessed due to missing or incomplete information.
1	Poor. The criterion is inadequately addressed, or there are serious inherent weaknesses.
2	Fair. The proposal broadly addresses the criterion, but there are significant weaknesses.
3	Good. The proposal addresses the criterion well, but a number of shortcomings are present.
4	Very Good. The proposal addresses the criterion very well, but a small number of shortcomings are present.
5	Excellent. The proposal successfully addresses all relevant aspects of the criterion. Any shortcomings are minor.

The score of a proposal will be determined by applying a weighted average of the score against each relevant award criterion, meaning that the individual score of a proposal will range from 0 to 5. Weights that will apply are:

- 2 for criteria 1, 4 and 6;
- 1 for criteria 2, 3 and 5.

The final assessment and score of a proposal will result from a consensus of the different experts' outputs. Proposals that will get a final consensus score below 3,3 points will be rejected.

Criterion 1. Contribution to excellence, in particular by showing that the proposal presents significant advantages over existing defence products or technologies

1.1 Quality of the proposed solution

- Description of the overall concept underpinning the project including the main ideas and technologies.
- Explanation of how your proposal addresses the specific challenge, scope, targeted activities, main high-level requirements and expected impact of that topic as set out in the call for proposals.
- Description and explanation of how the expected outcome of the action differs from and represents (or will represent in combination with other technologies) an advantage at strategic and/or technological, and/or defence operational level over existing defence products or technologies.
- If relevant for this criterion, explanation of how the proposed solution will provide an improvement in terms of the efficiency across the lifecycle in comparison to existing solutions, for example, by lower production, operational, maintenance, repair and overhaul or disposal costs as well as due to increased cost-effectiveness and the potential for synergies in the procurement and maintenance process.

1.2 Excellence in regards to the quality of the implementation, organisation and resources

- Description of the objectives of the proposal, which should be clear, measurable, realistic and achievable within the proposed duration. Describe the key milestones and deliverables of the project.
- Schedule and resource management of the proposed activities. If needed, justification of the allocation of time and resources.
- Provision of a presentation of the overall structure of the work plan (work breakdown structure) with the timing and inter-relations of the different work packages and their components (Gantt chart, Pert chart or similar).
- Description and explanation of the management processes, the organisational structure and the decision-making mechanisms, and their appropriateness to the complexity and scale of the project.
- Identification and assessment of the project specific critical risks, which could compromise the achievement of the stated project's objectives and detail of proposed risk treatments (*e.g.* mitigation measures).
- Description of the way each of the consortium members contributes to the project, how they complement one another (and cover the value chain, where appropriate) and of how the work share contributes to high levels of effectiveness and efficiency.
- If applicable, description of why third parties are involved in the action and in what way they contribute to the project.

Criterion 2. Contribution to innovation, in particular by showing that the proposal includes 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

- Description of the key innovative aspects of the project and explanation of to what extent the proposal contains ground-breaking or novel concepts and approaches, and/or new promising future technological improvements previously not applied in the defence sector. It must include an analysis of the Union’s internal market and the global market place.
- Explanation of how and to what extent the innovations/technologies developed under this proposal (with an exception to those contributing to increasing the efficiency across the lifecycle) could spin-off to other defence capabilities and if any patents are expected to be deposited under the project.
- If relevant, description and explanation of how the innovative solution proposed in the project will contribute to increasing efficiency across the lifecycle (*e.g.* by lower production, operational, maintenance, repair and overhaul or disposal costs) when applied to other defence capabilities. It must consider an increase in the cost-effectiveness and the potential for synergies in the procurement and maintenance process.

Criterion 3. Contribution to the competitiveness and growth of defence undertakings throughout the Union, in particular by creating new market opportunities

- Explanation of how the project will contribute to the improvement of the competitiveness of the European Defence Technological Industrial Base (EDTIB). Explanation of the foreseen competitive advantage of the product/technology/solution vis-a-vis existing or planned products/technologies/solutions both within and outside of the Union.
- Demonstration of the viability of the project by indicating the size and the growth potential of the market it addresses as well as expected volumes of sales both within and outside of the Union. Explanation of the impact that the project will have on the employment, turnover and investments in the EDTIB.
- If relevant, description and explanation of how the solution proposed in the project contributing to increasing efficiency across the lifecycle (*e.g.* by lower production, operational, maintenance, repair and overhaul or disposal costs) will create new market opportunities.

Criterion 4. Contribution to the industrial autonomy of the European defence industry and to the security and defence interests of the Union by enhancing defence products or technologies in line with defence capability priorities agreed by Member States within the framework of the Common Foreign and Security Policy, particularly in the context of the Capability Development Plan, and, where appropriate, regional and international priorities provided that they serve the Union's security and defence interests and do not exclude the possibility of participation of any Member State

- Explanation of how and to what extent the proposed action will contribute to the Union strategic autonomy by decreasing the Union's industrial and technological dependence from third countries regarding the targeted technology/capability.
- Description of the impact that the proposed activities will have on the European security of supply.
- Description of how and to which extent the project outcome will contribute to the defence capability priorities agreed by Member States within the framework of the Common Foreign and Security Policy, particularly in the context of the Capability Development Plan.

In order to verify the priorities spelled out in the Capability Development Plan, refer to the version releasable to the industry, which is available from the national defence associations or to the version available at:

https://www.eda.europa.eu/info-hub/publications/publication-details/pub/the-eu-capability-development-priorities.

- Description of, if applicable, to what extent the proposal does address a regional and/or an international priority that contributes to the Union's security and defence interests and does not exclude the possibility of participation of any Member State.

Criterion 5. The proportion of the overall budget of the action to be allocated to the participation of SMEs established in the Union bringing industrial or technological added value, as members of the consortium, as subcontractors or as other undertakings in the supply chain, and in particular the proportion of the overall budget of the action to be allocated to SMEs which are established in Member States other than those where the undertakings in the consortium which are not SMEs are established

Figures and SMEs listed in section 1 of Annexe 1 to the submission form will be taken into account for the evaluation of this award criterion[90].
For the call EDIDP-SME-2020, a score of 5 will be systematically given.

- Justification of the level of the allocation of the costs to the SMEs by explaining the specificity of the market and the features of the submitted proposal.
- Description and explanation of the industrial or technological added value brought by each of the SMEs established in the Union that has been listed in section 1 of Annexe 1.

Criterion 6. For actions covering:

- **the system prototyping of a defence product, tangible or intangible component or technology, or;**
- **the testing of a defence product, tangible or intangible component or technology, or;**

[90] The commitment in section 2 of Annexe 1 to the submission form is only relevant for the purpose of establishing the applicable funding rate bonuses and is not taken into account in the evaluation of the award criteria.

- **the qualification of a defence product, tangible or intangible component or technology, or;**
- **the certification of a defence product, tangible or intangible component or technology, or;**

contribution to the further integration of the European defence industry through the demonstration by the beneficiaries that Member States have committed to jointly use, own or maintain the final product or technology.
This criterion will not be taken into account for actions covering only studies, design and/or life-cycle technologies.

- In case the proposal covers activities referred to in points (c) to (f), provide supporting documents demonstrating how many Member States have committed to jointly use, own or maintain the final product or technology.
- Describe and explain how the above-mentioned commitments by Member States contribute to the integration of the EU market and increase the cooperation potential between Member States.

3.2.7. Selection criteria

Selection criteria are intended to assess the applicant's ability to complete the proposed action. Only proposals by applicants who satisfy the selection criteria may be considered for a grant. The necessary ability of the applicants will be assessed under both financial capacity and operational capacity, based on the information to be provided in the submission form and in the Participant register.

Financial capacity: the applicants must demonstrate that they have stable and sufficient sources of funding to maintain their activity throughout the duration of the grant and to participate in the funding of the action. This capacity will be verified in particular on the basis of the following supporting documents to be provided in the Participant register:

- balance sheet and profit & loss account for the last two financial years for which the accounts were closed;
- audit report produced by an approved external auditor certifying the above-mentioned accounts for applicants requesting more than EUR 750 000 of Union financial support.

Where a statutory audit is required by EU or national law, it must always be submitted. The audit report must certify the accounts for up to the last three available financial years. Where a statutory audit is not required, the applicant must provide a self-declaration signed by its authorised representative certifying the validity of its accounts for up to the last three financial years available.

The authorising officer responsible may, depending on a risk assessment, waive the obligation to produce the audit report for education and training establishments. The waiver is also possible in case of agreements with a number of beneficiaries who have accepted joint and several liabilities or who do not bear any financial responsibility.
In particular, supporting documents will not be requested for:

(a) natural persons in receipt of education support;
(b) natural persons most in need and in receipt of direct support;
(c) public bodies including Member State organisations;
(d) international organisations;
(e) persons or entities applying for interest rate rebates and guarantee fee subsidies where the objective of those rebates and subsidies is to reinforce the financial capacity of a beneficiary or to generate an income.

Operational capacity: the applicants must demonstrate that they have the professional competencies and qualifications required to complete the proposed action. This capacity will be assessed on the basis of information about specific qualifications, professional experience and references in the field concerned, to be provided with the proposal (see Annexe 7 to the submission form).

3.2.8. Ranking mechanism and award decision

For each call, assessed proposals will be ranked according to their final consensus score.

The proposal with the highest rank will be awarded.
Where a call mentions that several actions may be funded, the next proposals on the ranking list will also be awarded subject to the availability of budget and, where several topics are covered in the call, provided that these proposals address different topics (or different defence products, solutions, materials or technologies for the call EDIDP-SME-2020) from those already awarded.

The following approach will be applied successively for every group of *ex aequo* proposals requiring prioritisation, starting with the highest scored group, and continuing in descending order:

- Proposals that address topics not otherwise covered by more highly ranked proposals, will be considered to have the highest priority;
- These proposals will themselves be prioritised according to the scores they have been awarded for criterion 1 (contribution to excellence). When these scores are equal, priority will be based on scores for criterion 2 (contribution to innovation).

The Commission will adopt an award decision based on the ranking list (main and reserve list) after having consulted the Member States through the EDIDP Programme Committee. The adoption of the award decisions will be the starting point for informing the applicants and inviting awarded consortia to enter into grant agreement preparation (GAP) with the Commission.

For the highest ranked proposals on the reserve list, coordinators will be informed that their proposal may receive funding should budget still be available at the end of the GAP. In such case, they will be invited for negotiation on the scope and budget of their proposal.

3.3. Funding rates and Union financial contribution

The Union financial contribution will be calculated according to the mechanism described below.

3.3.1. Calculation mechanism

The maximum Union financial contribution will be calculated based on the total eligible costs provided and justified by the applicants at the time of submission of the proposal (see Annexe 2 to the submission form).
Indirect eligible costs must be determined by applying a flat rate of 25% of the total direct eligible costs, excluding direct eligible costs for subcontracting.
The costs listed in points a) to d) of paragraph 4 of Article 186 of the Financial Regulation will also be considered as eligible.
For more details and definitions of eligible costs, direct and indirect costs and subcontracting, please refer to the relevant sections of the guide for applicants.

The maximum Union financial contribution will be first calculated for each type of activity covered by the proposal (studies, design, prototyping, testing…), applying the baseline funding rates as described in section 3.3.2 to the eligible costs of the given activity. Where conditions are met, the baseline funding rate will be increased by an additional number of percentage points (bonus) as described in section 3.3.3. The overall bonus cannot exceed 35%.

For that purpose, the applicants must provide and justify eligible costs for each activity (see Annexe 2 to the submission form), keeping in mind the following rules:

- an activity may be broken down into several work packages;
- a work package must only cover one type of activity;
- the funding rate applicable to eligible costs of work package 1 (management and coordination of the project) must be the one for the activity "studies".

Applicants are invited to refer to the relevant section of the guide for applicants for more details about the information that needs to be provided.

The maximum Union financial contribution to the entire awarded action will be determined by adding up the maximum Union financial contribution calculated for each type of activity covered by the action.

The maximum Union financial contribution cannot exceed 100% of the eligible costs of the proposed action.

Applicants must request a Union financial contribution that is lower than or equal to the maximum Union financial contribution and that does not exceed the indicative budget allocated to the call.

3.3.2. Table 1. Baseline funding rates

Activity	Baseline funding rate
Studies, such as feasibility studies, and other accompanying measures	Up to 90% of eligible costs
The design of a defence product, tangible or intangible component or technology as well as the technical specifications on which such design has been developed, including partial tests for risk reduction in an industrial or representative environment	Up to 65% of eligible costs
The system prototyping of a defence product, tangible or intangible component or technology	Up to 20% of eligible costs
The testing of a defence product, tangible or intangible component or technology	Up to 65% of eligible costs
The qualification of a defence product, tangible or intangible component or technology	Up to 65% of eligible costs
The certification of a defence product, tangible or intangible component or technology	Up to 65% of eligible costs
The development of technologies or assets increasing efficiency across the life cycle of defence products and technologies	Up to 65% of eligible costs

3.3.3. Table 2. Additional number of percentage points (bonus) to the baseline funding rate listed in Table 1

Cumulated bonuses cannot exceed 35%.

Condition to be fulfilled to get the corresponding bonus	**Bonus** (additional number of percentage points to the baseline funding rate)
PESCO bonus	
Action developed in the context of the permanent structured cooperation (PESCO)	+ 10%
SME bonus	
Proportion of eligible costs allocated to SMEs established in the EU ≥ 10%	Proportion of eligible costs allocated to non cross-border SMEs established in the EU (up to maximum 5%) + Twice the proportion of eligible costs allocated to cross-border SMEs established in the EU
Mid-cap bonus	
Proportion of eligible costs allocated to Mid-caps established in the EU ≥ 15%	+ 10%

For the definition of SME, applicants must refer to EU Recommendation 2003/361[91].

'**cross-border SMEs established in the EU**' must be understood as SMEs established in Member States other than those in which the undertakings in the consortium that are not SMEs are established.
'**EU non cross-border SMEs established in the EU**' are SMEs established in the Member States in which the undertakings in the consortium that are not SMEs are established.
'Mid-cap' (or 'Middle-capitalisation company') means an enterprise that is not an SME and that has up to 3 000 employees, where the staff headcount is calculated in accordance with Articles 3 to 6 of the Annex to Recommendation 2003/361.

The applicability of the bonuses for SME/cross-border SME and mid-cap participation will be determined on the basis of the information provided in Annexe 1 to the submission form.

[91] Commission Recommendation C(2003) 1422 of 6 May 2003 concerning the definition of micro, small and medium-sized enterprises, OJ L 124, 20.5.2003, p. 36–41.

3.4. Duration of an action

Duration of the proposed action is not expected to exceed four years, unless duly justified in the proposal. In any case, duration of the proposed action must not exceed six years.

3.5. Consortium

Applicants must set up a consortium and appoint one of them to act as coordinator. The coordinator must be the principal point of contact between the members of the consortium in relations with the Commission. The coordinator will be identified in the grant agreement.

The members of a consortium participating in an action must conclude an internal agreement establishing their rights and obligations with respect to the carrying out of the action in accordance with the grant agreement. The internal agreement must also include arrangements regarding the intellectual property rights relating to the products and technologies developed.

3.6. Grant agreement

For each proposal selected for award, the coordinator of the consortium will be invited to enter grant agreement preparations with the Commission. A model grant agreement is available here.

The Commission may request additional information for the conclusion of the grant, such as those related to financial capacity, costs or legal status of future beneficiaries.

The attention of the applicants is drawn on the following points:

- Where Member States have appointed a project manager to lead the work related to the action that will received Union funding, the Commission must consult the project manager on the progress achieved in connection with the action before executing the payment to the eligible beneficiaries.
- In addition to the deliverables identified by the applicants in their proposal, specific periodic reports and a final report will be requested to the consortium in the grant agreement for the purpose of managing the grant. These reports must include a dedicated chapter containing data necessary for the monitoring and the evaluation of the Programme. The final report must in particular contain data necessary for the preparation of the evaluation report that the Commission is required to produce in line with the provisions of Article 17(2) of the EDIDP Regulation. This will include, for instance, data on cross-border participation, including of SMEs and mid-caps, in actions carried out under the Programme, as well as the integration of SMEs and mid-caps in the global value chain, information on the countries of origin of the beneficiaries and, where possible, the distribution of the generated intellectual property rights.

3.7. Actions involving the handling of classified information[92]

Pursuant to Commission Decision (EU) 2019/513 of 26 March 2019 on the security framework for the European Defence Industrial Development Programme, in case the implementation of the grant involves the handling of classified information, Member States on whose territory the beneficiaries are established must decide on the originatorship of the classified foreground information generated in the performance of an action. For that purpose, those Member States may decide on a specific security framework for the protection and handling of classified information relating to the action and must inform the Commission thereof. Such a security framework must be without prejudice to the possibility for the Commission to have access to necessary information for the implementation of the action.

If no such specific security framework is set up by those Member States, the security framework will be put in place by the granting authority in accordance with Commission Decision (EU, Euratom) 2015/444 on the security rules for protecting EU classified information ('Decision 2015/444'). Further details are provided in the Annexe to this document.

The applicable security framework for the action has to be in place at the latest before the signature of the grant agreement.

3.8. Additional conditions for the call EDIDP-SME-2020

The consortium applying for funding under call EDIDP-SME-2020 must be composed of small and medium-sized enterprises (SMEs) only. SMEs must be understood as defined in EU Recommendation 2003/361.

Applicants who want to know if they are SMEs according to this Recommendation must perform a self-assessment online on the Funding and Tenders portal.

SMEs members of the consortium will all be considered as cross-border SMEs.

Non-SMEs can participate in the action (whether as subcontractor or as non SME partner) but cannot be part of the consortium.

Please refer to the relevant section of the guide for applicants for more details.

Subcontracting will be strictly limited to 30% of the eligible costs of the action.

The Union financial support for a proposal cannot exceed EUR 2 500 000.

3.9. List of eligible countries

Public or private undertakings established in the following countries will be eligible to receive funding (*i.e.* become beneficiaries, linked third parties or subcontractors involved in the action) through EDIDP grants:

- The Member States (MS) of the European Union (EU), including their outermost regions.

The attention of the applicants is drawn on the existence of other eligibility criteria (please refer to section 3.2.5).

[92] Restricted and above.

Applicants are invited to read carefully the guide for applicants (available here) which provides additional guidance on how to fill the submission form and to prepare proposals.

Questions regarding the calls can be submitted by email at EC-EDIDP-proposals@ec.europa.eu. However, questions received after 1 November 2020 may not be answered by the Commission before the deadline for submission of the proposals. Any questions or replies do not constitute any ground to claim any expectation concerning the selection of the proposal or the award of the grant.

4. Annexe – Security aspects

4.1. Introduction

This Annexe issued by the European Commission – DG for Internal Market, Industry, Entrepreneurship and SMEs – mentions the main Security Aspects to complement the EDIDP call for proposals for 2020.

It establishes the general requirements for the performance of the tasks identified in the calls, which may involve the handling of classified information.

The beneficiary's National Security Authority (NSAs) is responsible for ensuring that the beneficiaries under their jurisdiction comply with the applicable security provisions for the protection of classified information.

4.2. Definitions

ACTION means, in the light of Regulation (EU) 2018/1092 of the European Parliament and of the Council of 18 July 2018 establishing the European Defence Industrial Development Programme aiming at supporting the competitiveness and innovation capacity of the Union's defence industry, the project selected under the Programme which the Consortium is to carry out.

BENEFICIARY is an individual or legal entity possessing the legal capacity to receive funding through a grant in the EDIDP and which has been selected by the Programme to receive the grant.

CLASSIFIED INFORMATION means any information or material designated by a security classification, the unauthorised disclosure or loss of which could cause varying degrees of prejudice to the interests of one or more of the Participants or any other State or international organisation with which the Participants have concluded a security of information agreement. Its classification level, and therefore the level of protection to be afforded to it by the recipient of the classified information, is indicated by a classification marking as detailed in the Appendix to this Annexe.

CONSORTIUM means a collaborative grouping of undertakings constituted to carry out an action under this Programme.

DESIGNATED SECURITY AUTHORITY (DSA) is a state authority responsible to the National Security Authority (NSA) of a participant which is responsible for communicating to industrial or other entities national policy on all matters of industrial security and for providing direction and assistance in its implementation. The function of DSA may be carried out by the NSA or by any other competent authority in that Participant state.

EU CLASSIFIED INFORMATION (EUCI) means any information or material designated by an EU security classification, the unauthorised disclosure of which could cause varying degrees of prejudice to the interests of the European Union or of one or more of the Member States.

FACILITY SECURITY CLEARANCE (FSC) means an administrative determination by a NSA, DSA or competent Security Authority that, a facility can afford an adequate level of protection to classified information to a specified security classification level.

FOREGROUND INFORMATION is classified information generated in the performance of the Action.

GRANTING AUTHORITY is the Commission department responsible for the Programme, which prepares, awards, cancels or modifies grant agreements.

NATIONAL SECURITY AUTHORITY (NSA) is a government authority with ultimate responsibility for the security of Classified Information in that country.

PERSONNEL SECURITY CLEARANCE (PSC) means a statement by a competent authority of a Participant state, which is made following completion of a security investigation conducted by a competent authority of a Participant state and which certifies that an individual is cleared to have access to Classified Information.

SECURED AREA is a physically protected area with a visibly defined and protected perimeter through which all entry and exit is controlled by means of a pass or personal recognition system, where unescorted access is granted only to individuals who are security cleared and are specifically authorised to enter the area on the basis of their need-to-know, and where all other individuals are escorted at all times or are subject to equivalent controls.

SECURITY ASPECTS LETTER (SAL) is a set of special contractual conditions, issued by the Contracting or Granting Authority, which forms an integral part of a Classified Contract or Classified Grant involving access to or generation of Classified Information, that identifies the security requirements or those elements of the contract or grant requiring security protection.

SUB-CONTRACTOR is a legal entity awarded a sub-contract under the Action.

4.3. General conditions

Pursuant to Commission Decision (EU) 2019/513 of 26 March 2019 on the security framework for the European Defence Industrial Development Programme, in case the implementation of the grant involves the handling of classified information, Member States on whose territory the beneficiaries are established must decide on the originatorship of the classified foreground information generated in the performance of an action. For that purpose, those Member States may decide on a specific security framework for the protection and handling of classified information relating to the action and must inform the Commission thereof. Such a security framework must be without prejudice to the possibility for the Commission to have access to necessary information for the implementation of the action.

If no such specific security framework is set up by those Member States, the security framework will be put in place by the granting authority in accordance with Commission Decision (EU, Euratom) 2015/444 on the security rules for protecting EU classified information (‘Decision 2015/444’).

The applicable security framework for the action has to be in place at the latest before the signature of the grant agreement.

The applicable security framework will be detailed in the Security Aspect Letter (SAL) which will be integral part of the Grant Agreement.

4.4. Access to classified information

All entities participating in grants which involve creation or access to information classified CONFIDENTIAL or SECRET, or at RESTRICTED level where requested by national rules, at the consortium's premises, must ensure that a valid Facility Security Clearance (FSC) at the appropriate level exists for the premises. This FSC must be granted by the National Security Authority (NSA/DSA) of the entity involved.

The involved entities must hold a duly confirmed FSC at the appropriate level. Until a Secured Area is in place and accredited by national NSAs, handling of classified information above RESTRICTED level must not be possible in their premises.

Access to and handling of classified information for the purposes of the Action must be limited to individuals with a need-to-know in possession of a valid Security Clearance.

Upon termination of the grant agreement when EUCI is no longer required for the performance of the grant, the Beneficiary must return any EUCI they hold to the contracting authority immediately. Where the Consortium is authorised to retain EUCI after termination or conclusion of the grant, the EUCI must continue to be protected in accordance with Commission Decision (EU, Euratom) 2015/444.

4.5. Marking of classified information

Classified information generated for the performance of the grant agreement must be marked in accordance with the applicable security instructions of the Action.

Grant agreements must not involve information classified ‘TRES SECRET UE/EU TOP SECRET’ or an equivalent classification.

4.6. Other provisions

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

All security breaches related to classified information must be investigated by the relevant security authority.

Appendix to Annexe - Table of equivalent security classification markings

Participant	Secret	Confidential	Restricted
EU	SECRET UE/EU SECRET	CONFIDENTIEL UE/EU CONFIDENTIAL	RESTREINT UE/EU RESTRICTED
Austria	GEHEIM	VERTRAULICH	EINGESCHRÄNKT
Belgium	SECRET (Loi du 11 Dec 1998) or GEHEIM (Wet van 11 Dec 1998)	CONFIDENTIEL (Loi du 11 Dec 1998) or VERTROUWELIJK (Wet van 11 Dec 1998)	DIFFUSION RESTREINTE or BEPERKTE VERSPREIDING *(Note, see below)*
Bulgaria	СЕКРЕТНО	ПОВЕРИТЕЛНО	ЗА СЛУЖЕБНО ПОЛЗВАНЕ
Croatia	TAJNO	POVJERLJIVO	OGRANIČENO
Cyprus	ΑΠΌΡΡΗΤΟ ABR:(ΑΠ)	ΕΜΠΙΣΤΕΥΤΙΚΌ ABR:(ΕΜ)	ΠΕΡΙΟΡΙΣΜΈΝΗΣ ΧΡΉΣΗΣ ABR:(ΠΧ)
Czech Republic	TAJNÉ	DŮVĚRNÉ	VYHRAZENÉ
Denmark	HEMMELIGT	FORTROLIGT	TIL TJENESTEBRUG
Estonia	SALAJANE	KONFIDENTSIAALNE	PIIRATUD
Finland	SALAINEN or HEMLIG	LUOTTAMUKSELLINEN or KONFIDENTIELL	KÄYTTÖ RAJOITETTU or BEGRÄNSAD TILLGÅNG
France	SECRET DÉFENSE	CONFIDENTIEL DÉFENSE	*(Note, see below)*
Germany *(Note, see below)*	GEHEIM	VS - VERTRAULICH	VS - NUR FÜR DEN DIENSTGEBRAUCH
Greece	ΑΠΌΡΡΗΤΟ ABR:(ΑΠ)	ΕΜΠΙΣΤΕΥΤΙΚΌ ABR:(ΕΜ)	ΠΕΡΙΟΡΙΣΜΈΝΗΣ ΧΡΉΣΗΣ ABR:(ΠΧ)
Hungary	TITKOS!	BIZALMAS!	KORLÁTOZOTT TERJESZTÉSŰ!
Ireland	SECRET	CONFIDENTIAL	RESTRICTED

Participant	Secret	Confidential	Restricted
Italy	SEGRETO	RISERVATISSIMO	RISERVATO
Latvia	SLEPENI	KONFIDENCIĀLI	DIENESTA VAJADZĪBĀM
Lithuania	SLAPTAI	KONFIDENCIALIAI	RIBOTO NAUDOJIMO
Luxembourg	SECRET LUX	CONFIDENTIEL LUX	RESTREINT LUX
Malta	SIGRIET	KUNFIDENZJALI	RISTRETT
Netherlands	Stg. GEHEIM	Stg. CONFIDENTIEEL	Dep. VERTROUWELIJK
Poland	TAJNE	POUFNE	ZASTRZEŻONE
Portugal	SECRETO	CONFIDENCIAL	RESERVADO
Romania	STRICT SECRET	SECRET	SECRET DE SERVICIU
Slovakia	TAJNÉ	DÔVERNÉ	VYHRADENÉ
Slovenia	TAJNO	ZAUPNO	INTERNO
Spain	RESERVADO	CONFIDENCIAL	DIFUSIÓN LIMITADA
Sweden	HEMLIG or HEMLIG/SECRET or HEMLIG	HEMLIG or HEMLIG/CONFIDENTIAL	HEMLIG or HEMLIG/RESTRICTED
United Kingdom	UK SECRET	No equivalent *(Note: see below)*	UK OFFICIAL - SENSITIVE

Notes:

Belgium and France: Both Participants handle and protect classified information bearing the marking “RESTRICTED” or equivalent according to its national laws and regulations in force for the protective level “DIFFUSION RESTREINTE” (also “BEPERKTE VERSPREIDING” in the case of Belgium) or the standards defined in the present document whichever is higher. The other Participants will handle and protect information marked “DIFFUSION RESTREINTE” (also “BEPERKTE VERSPREIDING” in the case of Belgium) according to their national laws and regulations in force for the level “RESTRICTED” or equivalent or according to the standards defined in the present document whichever is higher.
Germany: VS = Verschlusssache.
United Kingdom: The UK handles and protects classified information marked CONFIDENTIEL UE/EU CONFIDENTIAL in accordance with the protective security requirements for UK SECRET.