

European Defence Fund

2021 calls for proposals, conditions for the calls and annex

based on
Regulation (EU) 2021/697
and on
Commission implementing Decisions C(2021)4910 and C(2021)4897

v1.41

4 October 2021

HISTORY OF CHANGES			
Version	**Publication Date**	**Change**	**Page**
v1.00	30/06/2021		
v1.10	02/07/2021	- Removal of footer EN - Precision regarding the page limit for Part B Section 6 and 7 for Development actions	- all - 192
v1.20	20/07/2021	- Addition of the date of adoption of the 2021 EDF work programme - Precision added in reference to the Research calls - Update of the hyperlinks to *Submission forms* and *Guide for applicants* - Missing references to the lump sum approach for the call EDF-2021-DIS-RDIS - Precision regarding format of submission of completed forms and supporting documents. - Correction of inconsistency in the wording in i) and j) - Precision regarding specific conditions applicable to PRS related activities - Addition of references to definitions of SME and mid-cap - Precision regarding availability of the *Model Grant Agreements*	- 6 - 7 - 8, 213 - 163, 189, 206, 211 - 191 - 195 - 198 - 203, 209 - 211
v1.30	04/08/2021	- Replacement of “topics” by “solutions” (alignment with the work programme) - Corrigendum on the call topic ID EDF-2021-SPACE-D-SGNS (alignment with the work programme) - Clarification regarding the targeted type of applicants for the call EDF-2021-DIS-RDIS (alignment with the work programme)	- 13 - 51, 52, 197 - 163
v1.40	09/09/2021	- Corrigendum regarding the D nature of the call EDF-2021-ENERENV-D and associated topics (alignment with the work programme) - Update regarding the call for experts - Clarification regarding applicability of eligibility conditions to the entities involved in the action (footnote) - Clarification regarding eligibility of overseas countries and territories (OCTs) - Following the adoption of the decision of the EEA Joint Committee No 228/2021, amendment	- 9, 76, 185 - 9 - 186 - 192 - 193

		of footnote regarding participation of Norway - Alignment of wording and order of sections in the introduction of each call: o "Proposals are invited against [any of] the following topic[s]:" o Alignment of wording in the Budget section of each call - Addition of a headline and entry in the table of contents for the topic of each monotopic call - Correction of wrong cross-references to other sections of this document - Replacement of "linked third parties" by "affiliated entities" - Update regarding availability of the *Model Grant Agreements* - Clarification regarding zip archive - Addition of hyperlink to the PRS Decision and to the Space Programme Regulation - Update of hyperlinks - Harmonisation of formatting and of some wording across the whole document (impacts page numbering compared to previous versions) - Spelling and grammatical corrections - Call-specific meaningful updates: o In topic EDF-2021-MCBRN-D-MCM, removal of reference to "generating knowledge": content moved to "integrating knowledge" o In topic EDF-2021-PROTMOB-D-DMM, in "Targeted activities", replacement of "Action" by "Objective" to avoid misleading interpretation o In topic EDF-2021-DIS-RDIS-AMD, in Specific challenge, "proposals should ~~balance R&T efforts in~~ address R&T in one or more of the following areas:"	- each call cover page - each monotopic call - 9, 187 - 186 - 186, 208 - 188 - 194, 195 - 10, 185 - all - all - 17 - 146 - 173
v1.41	04/10/2021	- Alignment of wording regarding 40% limit for participation of research organisations to the call EDF-2021-OPEN-R - Alignement of wording regarding the 30% subcontracting limit for the calls EDF-2021-OPEN-R and EDF-2021-OPEN-D - Possibility to use the actual indirect costs regime for the lump sum grants approved	- 195 - 181, 183, 196 - 186, 203

Table of contents

1. INTRODUCTION 8

1.1. Implementation of the European Defence Fund (EDF) 8
1.2. Scope and content of the document 8
1.3. Key website 9
1.4. Reference documents 9
1.4.1. Basic texts 9
1.4.2. Documents needed to apply 10
1.4.3. Additional documents 10

2. CALLS 11

2.1. Call EDF-2021-MCBRN-R: Capabilities for CBRN risk assessment, detection, early warning and surveillance 11
2.1.1. Topic EDF-2021-MCBRN-R-CBRNDIM: Detection, identification and monitoring (DIM) of CBRN threats 12
2.2. Call EDF-2021-MCBRN-D: Defence medical countermeasures 15
2.2.1. Topic EDF-2021-MCBRN-D-MCM: Development of defence medical countermeasures 15
2.3. Call EDF-2021-C4ISR-D: ISR and advanced communications 18
2.3.1. Topic EDF-2021-C4ISR-D-HAPS: High-altitude platform systems 19
2.3.2. Topic EDF-2021-C4ISR-D-COMS: Robust defence multi-dimensional communications 23
2.4. Call EDF-2021-SENS-R: Optronics and radar technologies 28
2.4.1. Topic EDF-2021-SENS-R-IRD: Infrared detectors 28
2.4.2. Topic EDF-2021-SENS-R-RADAR: Advanced radar technologies. 31
2.5. Call EDF-2021-CYBER-R: Cyber threat intelligence and improved cyber operational capabilities 39
2.5.1. Topic EDF-2021-CYBER-R-CDAI: Improving cyber defence and incident management with artificial intelligence 39
2.6. Call EDF-2021-CYBER-D: Improved capacity for cyber training and exercises 45
2.6.1. Topic EDF-2021-CYBER-D-IECTE: Improved efficiency of cyber trainings and exercises 46
2.7. Call EDF-2021-SPACE-D: Resilient space-based PNT and SATCOM 52
2.7.1. Topic EDF-2021-SPACE-D-SGNS: Space and ground-based NAVWAR surveillance 52
2.7.2. Topic EDF-2021-SPACE-D-EPW: European protected waveform and accompanying technologies for resilient satellite communications against jamming 59
2.8. Call EDF-2021-DIGIT-R: Artificial intelligence 66
2.8.1. Topic EDF-2021-DIGIT-R-FL: Frugal learning for rapid adaptation of AI systems 67
2.9. Call EDF-2021-DIGIT-D: Cloud technologies 70

2.9.1. Topic EDF-2021-DIGIT-D-MDOC: Military multi-domain operations cloud 71
2.10. Call EDF-2021-ENERENV-D: Energy efficiency and energy management . 76
2.10.1. Topic EDF-2021-ENERENV-D-EEMC: Energy independent and efficient systems for military camps 76
2.10.2. Topic EDF-2021-ENERENV-D-NGES: Next generation electrical energy storage for military forward operation bases 82
2.10.3. Topic EDF-2021-ENERENV-D-PES: Alternative propulsion and energy systems for next generation air combat systems 85
2.11. Call EDF-2021-MATCOMP-R: Advanced materials and structures, and critical electronics 88
2.11.1. Topic EDF-2021-MATCOMP-R-PHE: Materials and structures for enhanced protection in hostile environments 88
2.11.2. Topic EDF-2021-MATCOMP-R-RF: Advanced RF components ... 91
2.12. Call EDF-2021-AIR-R: Next generation vertical take-off and landing systems 95
2.12.1. Topic EDF-2021-AIR-R-NGRT: Next generation rotorcraft technologies 95
2.13. Call EDF-2021-AIR-D: Avionics and advanced air combat 100
2.13.1. Topic EDF-2021-AIR-D-EPE: Enhanced pilot environment for air combat 101
2.13.2. Topic EDF-2021-AIR-D-CAC: European interoperability standard for collaborative air combat 107
2.14. Call EDF-2021-AIRDEF-D: Protection against high velocity aerial threats 114
2.14.1. Topic EDF-2021-AIRDEF-D-EATMI: Endo-atmospheric interceptor – concept phase 114
2.15. Call EDF-2021-GROUND-R: Precision Strike Capabilities 120
2.15.1. Topic EDF-2021-GROUND-R-IW: Improved warheads 121
2.16. Call EDF-2021-GROUND-D: Fleet upgrade and close combat 125
2.16.1. Topic EDF-2021-GROUND-D-FMGV: Future modular ground vehicles and enabling technologies, including green technologies . 126
2.16.2. Topic EDF-2021-GROUND-D-UGVT: Unmanned ground vehicle technologies 130
2.16.3. Topic EDF-2021-GROUND-D-3CA: BLOS collaborative close combat architecture 135
2.17. Call EDF-2021-PROTMOB-D: Soldier & logistic systems 140
2.17.1. Topic EDF-2021-PROTMOB-D-SS: Development of full-size demonstrators for soldier systems 140
2.17.2. Topic EDF-2021-PROTMOB-D-DMM: Development of a digital system for the secure and quick exchange of information related to military mobility 144
2.18. Call EDF-2021-NAVAL-R: Smart ships 149
2.18.1. Topic EDF-2021-NAVAL-R-DSSDA: Digital ship and ship digital architecture 149

2.18.2. Topic EDF-2021-NAVAL-R-SSHM: Ship Structural Health Monitoring 154
2.19. Call EDF-2021-NAVAL-D: Multirole and modular offshore patrol vessel . 156
2.19.1. Topic EDF-2021-NAVAL-D-MMPC: Modular and multirole patrol corvette 157
2.20. Call EDF-2021-DIS-RDIS: Research for disruptive technologies for defence applications 160
2.20.1. Topic EDF-2021-DIS-RDIS-QSENS: Quantum technologies for defence 160
2.20.2. Topic EDF-2021-DIS-RDIS-NLOS: Non-line-of-sight optical sensors applications 166
2.20.3. Topic EDF-2021-DIS-RDIS-OTHR: Over-the-horizon radars applications 169
2.20.4. Topic EDF-2021-DIS-RDIS-AMD: New materials and technologies for additive manufactured defence applications 172
2.21. Call EDF-2021-OPEN-RDIS: Open call addressing disruptive technologies for defence 178
2.21.1. Topic EDF-2021-OPEN-RDIS-OPEN: Research on disruptive technologies for defence 179
2.22. Call EDF-2021-OPEN-R: Open call focused on SMEs for research on innovative and future-oriented defence solutions 180
2.22.1. Topic EDF-2021-OPEN-R-SME: Research on innovative and future-oriented defence solutions 181
2.23. Call EDF-2021-OPEN-D: Open call dedicated to SMEs for development of innovative and future-oriented defence solutions 182
2.23.1. Topic EDF-2021-OPEN-D-SME: Development of innovative and future-oriented defence solutions 183

3. CONDITIONS FOR THE CALLS 185

3.1. Opening dates, final date for submission and indicative budgets 185
3.2. Evaluation procedure and conditions 186
3.2.1. Procedure 186
3.2.2. Indicative timeline for evaluation and grant agreement signature .. 187
3.2.3. Admissibility conditions 187
3.2.4. Exclusion grounds 189
3.2.5. Eligibility criteria 189
3.2.6. Ethics 196
3.2.7. Selection criteria 197
3.2.8. Award criteria and scoring 198
3.2.9. Ranking mechanism and award decision 202
3.3. Funding rates and Union financial contribution 203
3.3.1. Calculation mechanism 203
3.3.2. Applicable baseline funding rates 205
3.3.3. Additional number of percentage points (bonus) to the baseline funding rate (for development actions only) 206

3.3.4. Applicable maximum funding rates 207
3.3.5. Form of the grant 208
3.4. Duration of an action 208
3.5. Consortium 208
3.6. Grant agreement 208
3.7. Actions involving the handling of classified information 209
ANNEX ON SECURITY ASPECTS 211
1. Definitions 211
2. General conditions 212
3. Access to classified information 212
4. Marking of classified information 213
5. Other provisions 213

1. Introduction

1.1. Implementation of the European Defence Fund (EDF)

The objective of the EDF is to foster the competitiveness, efficiency and innovation capacity of the European defence technological and industrial base (EDTIB) throughout the Union, which contributes to the Union strategic autonomy and its freedom of action, by supporting collaborative actions and cross-border cooperation between legal entities throughout the Union, in particular SMEs and mid-caps, as well as by strengthening and improving the agility of both defence supply and value chains, widening cross-border cooperation between legal entities and fostering the better exploitation of the industrial potential of innovation, research and technological development, at each stage of the industrial lifecycle of defence products and technologies.

The proposals submitted against the EDF calls for proposals must be consistent with the defence capability priorities commonly agreed by Member States within the framework of the Common Foreign and Security Policy (CFSP), through:

- either collaborative research that could significantly boost the performance of future capabilities throughout the Union, aiming to maximise innovation and introduce new defence products and technologies, including disruptive technologies for defence, and aiming to make the most efficient use of defence research spending in the Union;
- or collaborative development of defence products and technologies, thus contributing to the greater efficiency of defence spending within the Union, achieving greater economies of scale, reducing the risk of unnecessary duplication and thereby fostering the market uptake of European defence products and technologies and reducing the fragmentation of defence products and technologies throughout the Union, ultimately leading to an increase in the standardisation of defence systems and a greater interoperability between Member States' capabilities.

The EDF is established by Regulation (EU) 2021/697[1] (hereafter, the EDF Regulation), which is implemented through annual work programmes and calls for proposals during the 2021-2027 multiannual financial framework.

The 2021 EDF calls for proposals are based on the 2021 EDF work programme defined in close cooperation with Member States and adopted by the Commission on 30 June 2021.

1.2. Scope and content of the document

This document contains the 2021 EDF calls for proposals, the conditions for the calls and an annex. It includes budgetary information, the criteria which the Commission will use to evaluate the proposals as well as other important information for applicants.

[1] Regulation (EU) 2021/697 of the European Parliament and of the Council of 29 April 2021 establishing the European Defence Fund and repealing Regulation (EU) 2018/1092, OJ L 170, 12.5.2021, p. 149-177.

In line with the 2021 EDF work programme, there will be 23 calls for proposals in 2021, among which:

- 19 thematic calls addressing 13 EDF categories of actions out of the 15 defined in the work programme
- one thematic call addressing research for identified disruptive technologies for defence applications
- three open calls among which one addressing disruptive technologies and two with a dedicated focus on Small and Medium-sized Enterprises (SME) as mentioned in the EDF Regulation in order to encourage further participation of such enterprises and foster innovation.

11 calls are targeting Research actions (EDF-2021-XXX-R[DIS]), including disruptive research, and 12 calls are targeting Development actions (EDF-2021-XXX-D).

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 annex to this document.

Finally, a dedicated call for expression of interest to establish a list of experts to assist the Commission with tasks in connection with EDF implementation for the period 2021-2027 has been launched (see here). 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"[2].

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].

[2] https://ec.europa.eu/info/funding-tenders/opportunities/portal/screen/programmes/edf.
[3] OJ L 193, 30.7.2018, p. 1–222.

[EDF Regulation] - Regulation (EU) 2021/697 of the European Parliament and of the Council of 29 April 2021 establishing the European Defence Fund and repealing Regulation (EU) 2018/1092[4].

[EDF Work programme 2021] - Commission implementing Decision C(2021) 4910 on the financing of the European Defence Fund established by Regulation (EU) N 2021/697 of the European Parliament and the Council and the adoption of the work programme for 2021.

[EDF Work programme 2022 – Part 1] - Commission implementing Decision C(2021) 4897 on the financing of the European Defence Fund and the adoption of the work programme for 2022 - Part I.

1.4.2. Documents needed to apply

This document and its annex.

The *Submission form* and its annexes (available here).

1.4.3. Additional documents

Guide for Applicants (available here).

The *Model Grant Agreement* and its annexes (available here after the opening of the calls).

[4] https://eur-lex.europa.eu/eli/reg/2021/697/oj, OJ L 170, 12.5.2021, p. 149-177.

2. Calls

The EDF calls for proposals for 2021 are described in this section.

2.1. Call EDF-2021-MCBRN-R: Capabilities for CBRN risk assessment, detection, early warning and surveillance

New and improved methods and technologies for the performant detection, identification and monitoring (DIM) of CBRN agents, as well as epidemics, emerging disease and pandemic influenza constitutes an important part of early detection and warning of infectious disease events[5] (biological hazards), chemical and radiological threats. CBRN early warning systems also collect, integrate, and inform military users, as well as relevant users in the health security sectors, about potential CBRN threats, epidemics, emerging diseases and pandemic influenza that can cause public health emergencies that undermine the full security of countries, from both natural or intentional origins.

Proposals must cover the generation of knowledge, methods and technologies leading to improved capacities for sampling, detection, identification, characterisation, monitoring as well as assessment of CBRN threats with a focus on biological agents, but not excluding chemical or radiological threats.

Activities should include but are not limited to innovative, technological improvements in detection technologies, notably regarding the quality of the basic input, *i.e.* data from sensors, methodologies and tools (or databases) for the identification and characterization of agents in complex bio-samples including sampling procedures, dynamic mapping of threats, vulnerabilities and capacities to respond at geographical levels, mapping of strategic CBRN detection technologies and related production capacities in Europe, agent classification and spread prediction based on artificial intelligence/machine learning, data processing, control measures, effectiveness of control measures and monitoring of their implementation in real-time, and use on mobile and field-based platforms (modular, scalable and adaptable).

Proposals are invited against the following topic:

- **EDF-2021-MCBRN-R-CBRNDIM:** Detection, identification and monitoring (DIM) of CBRN threats.

Budget

The Union is considering a contribution of up to EUR 18 500 000 to support proposals addressing the abovementioned topic and its associated specific challenge, scope, targeted activities and functional requirements.

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

[5] Decision No 1082/2013/EU of the European Parliament and of the Council of 22 October 2013 on serious cross-border threats to health defines 'epidemiological surveillance' as the systematic collection, recording, analysis, interpretation and dissemination of data and analysis on communicable diseases and related special health issues, OJ L 293, 5.11.2013.

2.1.1. Topic EDF-2021-MCBRN-R-CBRNDIM: Detection, identification and monitoring (DIM) of CBRN threats

Rapid detection of hazardous agents, detailed identification and monitoring over time and geographical area are an essential part of the CBRN response chain, and the demands vary depending on the specific task. Based on the situational awareness that DIM provides, military commanders can decide how to best proceed throughout their mission (whether the context is a military conflict or support to civilian society in a crisis situation). It is therefore crucial that the DIM system covers a broad range of CBRN-agents with an output of high reliability.

Performant CBRN DIM is not a single task using one technology or methodology. Existing technologies and their capabilities vary for DIM of biological, chemical, radioactive and nuclear substances. In a simplified manner, the order of technical and functional maturity level between the agent types can be described as B < C < RN.

The general challenges for performant DIM equipment (stand-off, point, integrated and/or personal worn, UxV, mobile devices or in critical infrastructures) are to address and improve performance parameters such as response time, sensitivity, selectivity, and false positive/false negative characteristics. Furthermore, the capability to detect, identify and characterize (un)known hazardous agents in a complex background need to be improved. Also, operational features such as robustness, size, mobility, power consumption and the possibility to widely and easily deploy/integrate the equipment into different surroundings and situations are of importance. In addition, sampling capability, for different matrices (air, water, soil, surfaces), as well as the ability to have a reliable chain of custody is required as an integrated part of the DIM process. Finally, the DIM equipment must be manageable by military personnel without scientific background.

Specific challenge

Several of the commonly used DIM technologies are based on collection of a large number of data (*e.g.* genetic and spectral data) that may need post processing and be interpreted or compared to library data bases in order to become useful. As potential threats continue to evolve and technology development proceeds, the data handling becomes more complex.

Specific challenges for B-DIM

A specific challenge with B-DIM is that microorganisms such as pathogenic viruses, bacteria, fungi and protozoa, or toxins, have to be detected or unambiguously identified in the presence of a high and varying natural non-pathogenic background. Stand-off and/or remote detection as well as continuous monitoring to trigger an alert for potential B threats is a challenge. Another challenge is the ability to identify rare and unexpected pathogens or organisms that have been (genetically) modified, which eludes certain specific identification methods.

Specific challenges for C-DIM

The capability of detecting low volatile C-agents on surfaces and corresponding aerosols needs to be improved. In particular, non-classical agents and new formulas for distributing agents requires new detection and identification methods and the adaption of existing ones.

The stand-off detection capability of vapour phase C-agents also needs improvement. In addition, toxins poses a challenge due to their diversity in size and physical properties.

Specific challenges for R-DIM

Detection and characterisation of nuclear detonations are important for early warning and fallout predictions in order to minimize consequences and preserve freedom of military action after the use of nuclear weapons. For this purpose, systems that can determine location, yield and type of nuclear detonation (*e.g.* air or surface burst) needs to be developed and refined. Possible methods that can be used are (but not limited to) seismic-, peak overpressure-, infrasound-, optical-, EMP- and initial radiation detection methods. For example, limitations that R-detection and monitoring instruments may suffer from lack of accuracy, or even overload at high counting rates needs to be overcome.

Scope

Proposals must cover the generation of knowledge, methods and technologies leading to improved capacities for sampling, detection, identification, characterisation, and monitoring of CBRN threats and data management. Proposals may also cover the dynamic mapping of threats, vulnerabilities and capacities to respond at geographical levels as well as mapping of strategic CBRN detection technologies and related production capacities in the Union. Considering maturity and current capabilities, the priority order is: prio 1: B-DIM; prio 2: C-DIM and prio 3: R-DIM. Proposals must cover one or several of the scopes described below.

To improve the decision making process, the quality of the basic input, *i.e.* data from sensors, needs to be significantly enhanced. Future detection devices need to target a broader spectrum of agents with higher sensitivity and selectivity at relevant response times, compared to existing devices. Their improved capability should preferably be demonstrated via benchmarking against current sensors as well as against agents of interest. The ability to rapidly detect hazards without sampling, preferably at safe distances, is desirable. The main scope of this call is development of technology and components (including algorithms for improved data extraction, risk assessment and spread prediction).

Methodology for identification and characterization of agents in complex bio-samples including sampling procedures also needs to be further developed. Methods that can initially provide indicative results for rapid response, but also provide data for deeper analysis such as characterization of properties of relevance for protection and treatment, as well as identification of previously uncharacterized agents, are preferred. Such deeper analysis can be done in the field or in specialized analysis reference centres. Development of tools (or databases) necessary for the characterization of non-standard or modified organisms and discrimination between natural/antagonistic origin of an outbreak is also required. As part of the DIM concept, sampling capability in different matrices should also be addressed.

Incorporations of novel and/or disruptive technologies is also encouraged, for instance, development of detectors on unconventional platforms and usage of AI for agent classifications. It is essential that the research activities generates new and improved DIM capability according to requirements generated from the operational need of the MS military forces. There is a specific need to reduce logistics in military operations, so next generation

CBRN DIM systems should strive towards being mobile, fieldable, modular, scalable and adaptable to the nature of the mission. Also the system should be user-friendly and be as autonomous as possible. Handling must not be entirely dependent on personnel with a scientific background.

The interpretation of comprehensive DIM data into assessments of risk areas, mapping of strategic CBRN capacities and other decision making processes requires development of advanced methods to interpret and present the information (*i.e.* virtual reality/augmented reality, real-time data fusion methodologies, uncertainty analyses and dispersion model protocols). In addition, methods for background signal discrimination and prediction of potential dissemination source have to be improved.

In order to achieve utilization and adaptation of the latest scientific developments, realization of the technology into products and to ensure applied usage of the systems, several partners are required. It must be outlined in the project proposal how the active involvement from industry, defence research organisations and academia as well as end users will be achieved.

Targeted activities

The proposals must cover the following activities as referred in Article 10(3) of the EDF Regulation, not excluding possible downstream activities eligible for research actions if deemed useful to reach the objectives:

- activities aiming to create, underpin and improve knowledge, products and technologies, including disruptive technologies, which can achieve significant effects in the area of defence;
- activities aiming to increase interoperability and resilience, including secured production and exchange of data, to master critical defence technologies, to strengthen the security of supply or to enable the effective exploitation of results for defence products and technologies.

The proposals must substantiate synergies and complementarity with foreseen, ongoing or completed activities in the field of CBRN DIM, notably through EU funded actions under Horizon 2020 and Horizon Europe or in the framework of the European Defence Agency.

Functional requirements

According to important performance indicators, an enhanced discrimination of threats from false targets with minimization of false alarm rates and identification of the type of threat is required.

It is essential that the research activities in this topic generates new or improved DIM capability according to requirements generated from the operational need of the MS military forces (*i.e.* agent range and formula, detection level, response time and selectivity) aiming towards autonomous mobile and field-based DIM systems.

Final adaptation to physical requirements regarding for instance mobility, size/miniaturization, weight, power consumption, networking, platform integration, situational awareness capability and general robustness is not excluded, but more suited for a

development program phase. Nevertheless, the proposals should include considerations on how the technology development can be driven with these parameters in mind.

Expected impact

Activities should serve as a solid foundation for the European defence research industry to build upon independently from external sources (IP, components and the product or service itself). The expected impact has multiple faces; security and defence of the society being the most obvious ones, but it brings significant strategic and economic benefits for the industry and employment within the EU.

The expected results should provide substantial improvements to the CBRN defence domain for the protection of troops, security forces as well as the population and critical infrastructure in general. Deployment of new DIM systems with improved functional capability will be more widely adopted throughout different levels within the armed forces (not only by specialist troops).

2.2. Call EDF-2021-MCBRN-D: Defence medical countermeasures

Defence medical countermeasures (MCMs) must be kept up-to-date, available and able to respond to the continuously changing and novel health threats posed by CBRN. MCMs may include any medicines or medical devices aimed to combat CBRN threats. This extends to countermeasures that prevent or treat the threat, but also to countermeasures that combat novel modes of delivery of such threats.

Proposals should focus on innovation and development of MCMs or an additional integration into military intelligence and information systems and corresponding civil capacities. Proposals are encouraged to provide for an analysis into novel MCMs and related technology, analysis of gaps and recommendations to ensure baseline preparedness standards and indicators, mapping of CBRN MCM capacities across EU, as well as options for ensuring EU's access and availability of MCMs.

Proposals are invited against the following topic:

- **EDF-2021-MCBRN-D-MCM:** Development of defence medical countermeasures.

Budget

The Union is considering a contribution of up to EUR 50 000 000 to support proposals addressing the abovementioned topic and its associated specific challenge, scope, targeted activities and functional requirements.

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

2.2.1. Topic EDF-2021-MCBRN-D-MCM: Development of defence medical countermeasures

Defence medical countermeasures (MCMs) must be kept up-to-date, available and able to respond to the continuously changing and novel health threats posed by CBRN. MCMs may include any medicines or medical devices aimed to combat CBRN threats. This extends to

countermeasures that prevent or treat the threat, but also to countermeasures that combat novel modes of delivery of such threats.

Proposals should focus on innovation and development of MCMs or an additional integration into military intelligence and information systems and corresponding civil capacities. Proposals are encouraged to provide for an analysis into novel MCMs and related technology, analysis of gaps and recommendations to ensure baseline preparedness standards and indicators, mapping of CBRN MCM capacities across EU, as well as options for ensuring EU's access and availability of MCMs.

Specific challenge

In recent years, chemical, biological and radiological threats have been continuously rising. For example, one cannot ignore the fact that groups/nations in the future might use disease-promoting microbes and viruses to damage a country's society or weaken its defence. The objective of proposals under this call is to update and/or develop medical countermeasures (MCMs) for the armed forces of EU and – wherever applicable – related civil/health protection to respond to the continuously changing and novel health threats posed by CBRN. It thus aims at developing shared capabilities for EU armed forces against CBRN crises generated by a natural or provoked event, and to treat pathologies or injuries of significant impact. It will thus contribute to responding more efficiently to conflicts, crises, or isolated events involving CBRN situations. Such MCMs should continue to be bolstered by both academia and industry within the EU due to:

- their specificity;
- the large funding to be engaged for R&D and poor market prospects;
- the low occurrence of such threats even though proliferation is increasing worldwide (thus increasing operational risks for armed forces);
- the large funding to be engaged for preclinical and clinical trials;
- the large scope of threats to be considered and final demand of the medical countermeasure.

Scope

Proposals should focus on innovation and development of MCMs against CBRN threats as well as their integration into armed forces. Proposals may also provide for analysis of the relevance and feasibility of novel MCMs and related technology, mapping of CBRN MCM capacities across EU, as well as options for ensuring EU's access and availability of MCMs.

MCMs[6] may include any medicines or medical devices that are aimed at combating CBRN threats. This extends both to countermeasures that prevent or treat the threat.

[6] Decision No 1082/2013/EU of the European Parliament and of the Council of 22 October 2013 on serious cross-border threats to health defines MCMs as medicines, medical devices and other goods or services that are aimed at combating serious cross-border threats to health, a life- threatening or otherwise serious hazard to health of biological, chemical, environmental or unknown origin, which spreads or entails a significant risk of spreading across countries, OJ L 293, 5.11.2013.

For MCMs to be updated, available and able to respond, this entails a large scope covering innovation, development and analysis.

Targeted activities

The proposals must cover the following activities as referred in Article 10(3) of the EDF Regulation, not excluding possible upstream and downstream activities eligible for development actions if deemed useful to reach the objectives:

- studies, such as feasibility studies to explore the feasibility of new or improved technologies, products, processes, services and solutions;
- the design of a defence product, tangible or intangible component or technology as well as the definition of the technical specifications on which such design has been developed which may include partial tests for risk reduction in an industrial or representative environment.

Integrating knowledge, testing, qualification, and certification of MCMs, as defined below, are desirable. Given that they concern CBRN MCMs, these activities are specific and should be understood, *e.g.* for immunotherapies, as:

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

Innovative disruptive technologies, like MCMs that limit the development of resistance (*e.g.* broad-spectrum MCMs), and platforms for local production of MCMs on-demand, are warranted.

Functional requirements

It is essential that the development activities in this topic generate new or improved medical countermeasure capabilities that are in alignment with requirements from the Member States

(MS)' armed forces themselves, or in combination with the operational needs of related civil protection or health authorities. According to the recommendations of national or European regulatory agencies, efficacy of the MCMs should be demonstrated on animal models as close as possible to humans – such as swine or non-human primates – during preclinical studies. MCMs may be developed from early technology readiness levels and, for most advanced products, up to GMP production, clinical trials, and certification for use in humans. Safety must be demonstrated in human volunteers during phase I clinical trials. The final product should be able to be administered in field conditions by trained medical personnel.

MCMs address the three letters C, B, and R, in the CBRN term:

- **chemical threat (C)** MCMs against severe poisoning by any chemical agent as indicated in the Chemical Weapons Convention, especially nerve agents;
- **biological threat (B)** MCMs against B agent for which classical treatments (*e.g.* antibiotics) are not available or not sufficiently efficient;
- **radiological threat (R)** MCMs against ionizing radiation effects like Acute Radiation Syndromes.

Expected impact

Proposals are expected to:

- provide substantial improvements to the CBRN defence domain for EU armed forces with consistent CBRN medical protections against a large panel of threats currently not covered by drugs produced within EU;
- facilitate the development of CBRN defence capabilities that each Member State, individual government or industry cannot face alone;
- develop EU autonomous industrial segments;
- contribute to the EU strategic autonomy.

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

2.3. Call EDF-2021-C4ISR-D: ISR and advanced communications

Proposals are invited against any of the following topics:

- **EDF-2021-C4ISR-D-HAPS:** High altitude platform systems;
- **EDF-2021-C4ISR-D-COMS:** Robust defence multi-dimensional communications.

Budget

The Union is considering a contribution of up to EUR 70 000 000 to support proposals addressing any of the abovementioned topics and their associated specific challenge, scope, targeted activities and functional requirements.

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

2.3.1. Topic EDF-2021-C4ISR-D-HAPS: High-altitude platform systems

Information superiority is a critical capability to be developed and improved with the aim to address future challenges to be faced by European Defence Forces and NATO stakeholders, and more specifically to support reactive and efficient decision-making processes. In order to improve systems dealing with command, control and communications (C3) capabilities, as well as Intelligence, surveillance and reconnaissance (ISR) capabilities, emergent technologies should be considered to enhance ISR and CIS operational availabilities, through persistence, acquisition of high quality data, automatic airborne processing and dissemination of information to relevant stakeholders.

While current observation satellites provide daily revisit frequency and upcoming constellations of small satellites propose a revisit time within an hour, this frequency will still be too low to understand properly the behaviour of a terrestrial, maritime or air target, and to track it. Stratospheric persistent airborne systems or High Altitude Platform Systems (HAPS) are particularly suitable to reach persistence, as environmental conditions are stable and allow continuous operations with limited meteorological impacts, thus contributing to high-availability operational requirements.

With respect to terrestrial and satellite networks, technical advantages provided by HAPS are numerous, among which:

- better propagation conditions for connectivity, lower latency, better sensor resolution;
- ability to remain continuously and persistently in an area for a long period.

HAPS, operating in the stratosphere, can provide an efficient solution to European Defence Forces, featuring simultaneously a capacity of permanence and endurance over a large area. HAPS can complement the surface, airborne and satellite systems for the surveillance and monitoring services, *e.g.* keeping a stationary position (at a first approximation) with respect to the ground and thus acting like a fixed observation platform. They provide unique performances in terms of resolution and/or link margin thanks to its relative proximity to the ground. They can provide over the horizon detection capabilities of ground, sea or low altitude air targets. Furthermore, the deployment and operation of multiple different sensors providing different types of data that will deliver high quality and valuable information when fused can strongly improve the relevance of such HAPS.

HAPS development projects can benefit from improvements in composite materials, low-power computing, battery technology and solar panels technologies, available in Europe. Main HAPS mission profiles are:

- broadband net nod, facilitating regional communication particularly among command posts;
- surveillance/airborne early warning, offering down to ground level month-long uninterrupted long range detection;
- persistent threat detection both for terrestrial and maritime surveillance, providing moving target indicator, imagery (EO/IR/SAR) or even detection of muzzle flashes, shockwaves or impact of the ammunition (rockets, artillery, mortar);

- SIGINT/ESM, detecting and analysing electronic emissions over long distances;
- communication cell node, offering a central management node designed for short range at line-of-sight propagation.

Specific challenge

The development of HAPS solutions necessitates solving specific technological, industrial and operational challenges:

- development of the concept of operation of such innovative assets integrated with other capabilities (including HAPS);
- maturity of the key technologies required to develop such persistent platforms;
- adaptation of platform materials, electronics and payloads to the stratosphere environment and high altitude position;
- real time processing of the data flow and data fusion both on board, and ground-based to maximize HAPS efficiency, or to integrate it into C4ISR architecture;
- integration in airspace during critical phases and respect of airspace sovereignty.

Scope

The proposals must aim to validate HAPS solutions, developing at least two different flight demonstrators of different kinds[7] to test properly the operational and technical challenges of the different HAPS platform types, and as such making a substantial contribution to European Defence and Security applications.

The proposals must include in particular:

- definition of the Concept of Operations of HAPS solutions in their various missions, taking into account their specific operational capacities. Such CONOPS will be used to design the prototypes or the new HAPS solutions (platform and payloads, including data processing);
- demonstration of the various HAPS demonstrators (platforms and payloads) to de-risk the key technologies and highlight the operational performances that can be expected from each demonstrator type;
- study of current and foreseen technology status and identification of road maps for each demonstrator involved.

Targeted activities

The proposals must cover the following activities as referred in Article 10(3) of the EDF Regulation, not excluding possible upstream and downstream activities eligible for development actions if deemed useful to reach the objectives:

- studies, such as feasibility studies to explore the feasibility of new or improved technologies, products, processes, services and solutions;

[7] Either non-propelled aerostats, propelled aerostats, hybrid platforms (*i.e.* both aerodynamic and aerostatic), solar powered aerodynes, or other aerodynes.

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

In particular, the proposals must cover the in-flight demonstrations of at least two high-altitude demonstrators (platform and mission) of different kinds[2] and the preliminary phases of the design of the HAPS products and associated mission systems, including in particular:

- design and realization of high-altitude platform demonstrators, design and realization of various missions from communication relay to surveillance/threat detection, including features of data acquisition and processing, the flight tests of the demonstrators including operational payload and the related conclusions in terms of key technologies and operational interests and benefits;
- CONOPS definition, system specifications, detailed requirements review (DRR) and architecture definition of the European HAPS capacities.

The proposals can also include the potential development of specific laboratory technological demonstrators, in order to support decision making during the design phase.

A detailed planning of possible further development phases will also be provided, including the identification of implementation priorities, according to operational needs of EU and Member States. Subsequent phases up to operational readiness should include in particular prototype development, qualification and test activities.

Functional requirements

For each of the HAPS platforms concerned, the proposals must meet the following main functional requirements in order to meet Defence needs:

- high altitude of operation (stratospheric layer, typically between 18 000 and 25 000 m) to ensure operational flexibility with respect to weather conditions;
- permanence, necessary to detect critical threats, with sufficient freedom of evolution to reach operational areas and follow battle rhythm;
- endurance with the objective to stay in flight at least for one month and up to one year, but lower endurance has to be compensated by higher capacity for the related platform to be rapidly deployed, even from not prepared terrains. Ability to support operations without limitation throughout their duration must be investigated;
- no ground logistical impact on the operational theatre;
- a powerful and diversified payload capacity, including telecommunication services and long range sensors, such as powerful imagery and radars, electronic and signal sensors, necessary for ISR missions (terrestrial, aerial or maritime);
- capacity to be relocated or deployed over foreign theatres;
- capacity to embark diverse payloads, according to the mission and to the user requirements, thanks to a modular design and a standardized interface (plug and play),

including towards the data management system. Each Member State can define its own payload, based on its own sensors. This capacity will be demonstrated by swapping payloads for diverse purposes and diverse origins;

- capacity to address mission profiles previously described (*cf.* specific challenge);
- capacity for the HAPS to be networked either with other HAPS or with other ISR platforms in order to increase the operational impact and resilience if needed;
- telecommunication applications, embarking a suitable telecommunication relay for ground, naval and aerial forces, and SATCOM relay;
- ability to transfer imagery and signal data collections to reach back centres like processing, exploitation and dissemination cells, potentially with the help of artificial intelligence must be investigated;
- ability to be easily integrated in current and foreseen C2 systems;
- electromagnetic and cyber resilient platform and payloads: only authorised parties must be allowed to take control of the system or to access information to and from the platform.

Expected impact

- Convincing demonstrations of the potential of various HAPS configurations in support of EU critical defence and security solutions.
- Cartography of technologies and systems effectiveness based on common key performance indicators.
- Ensure reliable, secure and autonomous availability of high performance and (re)configurable permanent surveillance solutions to military end-users.
- Provide flexibility for telecommunication and ISR aspects, which go beyond capabilities of satellites.
- Payload development and breakthrough on-board data processing technologies.
- Improvement of situational awareness, resilience and security of operations.
- Reduction of the personnel footprint and the global cost of military operations.
- Contribute to strengthening the European industry and help improve its global position through the development of innovative technologies along a new European manufacturing value chain.
- Supporting European Union industrial competitiveness by allowing development of innovative technologies in the framework of multiple emergent industrial domains such as aerospace, energy management, payload development, digital technologies and defence and security sector.

2.3.2. Topic EDF-2021-C4ISR-D-COMS: Robust defence multi-dimensional communications

Information superiority is key to achieve operational advantage against the enemy. Today, EU Member States (MS) armed forces use a variety of specialised communication means to coordinate and share relevant information during operations. In the tactical domain, to comply with the very demanding environment in high-intensity combat, radio communications systems have been designed with advanced mechanisms for discrete and robust communications, which results in limited data rate capabilities.

Current tactical data links and communications systems have operational and coalition limitations including vulnerabilities that need to be addressed. Wideband and reliable communication for operational interoperability, mobility and security that is robust against detection, acquisition and jamming are key capabilities for defence operations and electronic warfare, including far from the battlefield. However, robust, resilient and performant communications and software defined network architectures will be key features to build and deploy next generation military communication systems.

In the context of collaborative warfare, sensors' data must be shared and collectively analysed, including by means of big data analytics and artificial intelligence, in view of an efficient operational decision-making. This requires *ad-hoc*, any to any, ubiquitous, broadband, secured and low latency connectivity, which 5G technology could provide in certain operational scenarios.

An integrated tactical 5G bubble could offer a complementary and interoperable broadband capacity at the tactical level to increase information sharing, possibly speeding up the deployment of command posts, enhancing intelligence, surveillance and reconnaissance (ISR) data sharing and contributing to improve bases' logistics and security.

Therefore, it is needed to study 5G technologies with the target to integrate them (or a subset) in tactical CIS (Communication and Information Systems) to supply additional capabilities supporting specific missions and operational scenarios. A standardized and interoperable joint communication system or network is needed. Industry already has formulated flexible standards, like 5G and SDN[8] solutions and network architectures potentially based on software-driven approaches, edge computing and slicing, that pave the way for next generation networks.

Specific challenge

The specific challenge of this topic is to assess identified use cases, whereby 5G will bring improved operational capacities and build corresponding interoperable 5G solutions matching the military constraints in terms of robustness, resilience, security, sovereignty and manageability, and at the same time ensuring efficient interoperability of the 5G solutions with military networking technologies.

[8] Software defined network.

Scope

The proposals must address the development of a LTE[9]/5G integrated tactical bubble based on a robust defence multi-dimensional communication design, using commercial and military secure hardware, software and architecture, digital transceivers, considering multi-functional digital antenna systems, all with a SWaP-C (Size, Weight and Power - Cost) approach.

In particular, the proposals must lead to the identification and assessment of operational use cases where 5G will bring benefits, analyse the merits, the implementation guidelines, including eventual modifications, and prototype selected use cases, and the area of hardening, if necessary, will be identified and the militarisation/customization tasks will be further defined and assessed. The objective is to help optimising the 5G solutions for the intended military user taking care of the best combination of operational constraints and available 5G computing power.

The proposal must provide tested solutions covering all aspects from devices, infrastructure, security and orchestration of the overall system providing an optimized solution, in order to best integrate 5G solutions with other military network types that might be present in the use cases.

Among others, examples of potential military 5G use cases should possibly consider to:

- provide secure and robust command, control and communication providing information relevant at C2 (Command and Control) level for ISR and, in the future, for cyber situational awareness;
- remotely control unmanned vehicles and robots *e.g.* for surveillance and reconnaissance information;
- integrate 5G network enabling augmented/virtual reality for mission planning, training and operational use;
- integrate 5G network enabling smart warehouses, smart field health care and supply/logistic solutions.

Targeted activities

The proposals must cover the following activities as referred in Article 10(3) of the EDF Regulation, not excluding possible upstream and downstream activities eligible for development actions if deemed useful to reach the objectives:

- studies, such as feasibility studies to explore the feasibility of new or improved technologies, products, processes, services and solutions;
- the design of a defence product, tangible or intangible component or technology as well as the definition of the technical specifications on which such design has been developed which may include partial tests for risk reduction in an industrial or representative environment;

[9] Long Term Evolution.

- the development of a model of a defence product, tangible or intangible component or technology, which can demonstrate the element's performance in an operational environment (system prototype);
- the testing of a defence product, tangible or intangible component or technology.

The proposals must address in particular the following objectives:

Studies:

- EU Member States defence forces use case analysis for Homeland defence and Expeditionary operations with an emphasis on interoperability (land, maritime and air domains);
- evaluation of 5G standard and SDN systems to answer to the different use cases (including gap analysis) and new operational concepts (*e.g.* tactical cloud);
- analysis of concepts for adoption of an appropriate industry standard to military needs of EU Member States;
- definition of requirements for 5G military systems, considering also interoperability with other military radio networks;
- study on how to combine 5G systems with other network types that might be present in an operation;
- analysis on use case needs according to 5G system constraints to select underlying network architectures;
- analysis on how to improve cyber-resilience capabilities and, in general, 5G robustness against detection, acquisition and jamming (*e.g.* using *ad-hoc* resources management procedures, specialized antenna systems);
- presentation of the study results and execution of a demonstration with use cases, also to permit to evaluate the gaps in the 5G technologies for a secure integration with the tactical networks.

Design:

- definition of 5G solutions (including tactical bubbles) and SDN solutions applicable to centralised and distributed systems;
- definition of the system architecture, subsystems and interfaces, and guidelines for implementations, *etc*.), considering also interoperability with other military radio networks;
- definition of the security environment and solutions, considering secure overlays exploiting existing military standards;
- selection of a subset of use cases for demonstration, simulation and prototyping;
- definition of the scope for adoption of an appropriate industry standard to military needs;
- definition of the system architecture for adoption of an appropriate industry standard to military needs;

- definition of a testbed for the adoption of an appropriate industry standard to military needs;
- a proposal for potential subsequent projects that should be generated according to the operational needs of the EU Member States.

Prototyping for implementation of selected use cases (to be consolidated along the implementation):

- development of a prototype consisting in multiple integrated tactical bubbles in military networks including demonstration and/or prototyping of different interoperable tactical bubbles and end-to-end tactical networking, also integrated with military assets;
- presentation, if possible, of the study results and execution of a demonstration with use cases.

Testing:

- testing of the supported operational capabilities and present solutions for life cycle management, with the aim of increasing efficiency and cost-savings.

Functional requirements

The proposed solutions must fulfil the following requirements:

- utilising 3GPP[10] 5G standards (NR[11], 5GC[12], slicing, FWA[13]);
- 5G stand-alone solution;
- redundancy and security needed for critical solutions. Especially solutions considering the needs in terms of confidentiality, integrity and availability, when facing threats (including cyber threats) corresponding to the military use cases for 'active cyber defence';
- interoperability and integration with existing military infrastructure;
- low EMC[14] impact;
- implementation in a highly regulated spectrum;
- support for multi-dimensional operations;
- flexibility in network design leading to differentiated services in rapidly changing levels of conflict;
- leveraging commercial 5G networks for certain use cases;
- SWaP for the different use cases;
- ease/rapidity of deployment and associated tools (orchestration);
- low maintenance solutions, for long-term deployment;

[10] 3G Partnership Program, Global Standardization organization for the Mobil standards 3G, 4G, 5G and 6G.
[11] New Radio, the new radio optimized for mid- and high band radio spectrum specified by 3GPP.
[12] 5G Core Network.
[13] Fixed Wireless Access – the use case replacing fibre to homes and offices.
[14] Electromagnetic compatibility.

- interconnection of sensor technologies;
- human factor integration (HFI);
- interface for integration in mobile control units;
- robustness in design, including radio silence within seconds, broadcasting downlink without disclosing the receiver, millimetre waves usage, flexible/self-configuring network design and backhaul;
- support for geofencing[15].

Expected impact

The long-term effects should benefit a future strong, competitive and innovative technical and industrial defence development within EU Member States, by contributing to sovereignty, security of supply and security. In particular, the expected impacts are:

- to allow command entities to base their decisions on suitable timely and accurate information and to be able to transmit information swiftly and securely to relevant actors. This includes command, control and communication (C3), intelligence, surveillance and reconnaissance (ISR), sensors and electronic warfare;
- to reduce the cost for European military missions through verified knowledge of using COTS [16] /MOTS [17] products in civil and peacekeeping defence environments, thus to increase efficiency and cost-saving across the life cycle and benefit from cost;
- to create a European reference for standardised Tactical bubbles and hybrid SDN technologies for interoperability of SDN solutions that will improve the capabilities of the European defence industry to develop and supply state-of-the-art communication solutions;
- to reinforce interoperability of EU Member States armed forces, interoperability of SDN solutions with NATO FMN[18] initiative;
- to contribute to an increased EU military autonomy in this strategic area, where major actors are heavily investing;
- to create a European ecosystem platform for secured 5G devices and infrastructures, including hybrid networks (utilizing both civilian and military radio technologies), configuration and management tools and cyber security fit for military use;
- demonstration of adaption of an appropriate industry standard to military needs.

[15] Geofencing is the use of the global navigation satellite system (GNSS) and/or local radio-frequency identifiers (such as 5G radio base stations, Wi-Fi nodes or Bluetooth beacons) to create virtual boundaries around a location.
[16] Commercial off-the-shelf, using standard products and software, rather than customer tailored products. Benefitting the purchasing organisation.
[17] Military making use of COTS (and the high development pace of consumer products).
[18] North Atlantic Treaty Organization's Federated Mission Networking.

2.4. Call EDF-2021-SENS-R: Optronics and radar technologies

Proposals are invited against any of the following topics:

- **EDF-2021-SENS-R-IRD:** Infrared detectors;
- **EDF-2021-SENS-R-RADAR:** Advanced radar technologies.

Budget

The Union is considering a contribution of up to EUR 38 000 000 to support proposals addressing any of the abovementioned topics and their associated specific challenge, scope, targeted activities and functional requirements.

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

2.4.1. Topic EDF-2021-SENS-R-IRD: Infrared detectors

The domain of Infrared (IR) detectors encompasses a variety of technologies that detect in different spectral bands for a variety of applications (land, air, naval, space, missile guidance, drones…). IR detectors are key drivers to increase DRI[19] ranges and thus improve the global efficiency of the system (situation awareness and targeting).

Europe has a strong position in advanced military IR components and systems. Yet the risks are high that the Union becomes severely dependant on suppliers established in third countries for this critical defence technology in the medium/long term. This not only limits the strategic autonomy of the Member States but also generates security of supply risks.

It is key for Europe sovereignty to have a full "EU autonomous" supply chain of IR detectors. To achieve advanced performance of future IR systems in relevant platforms improved IR detectors with reduction of size, weight, power and cost is mandatory. The performance of the IR detector modules is driven not only by the IR detector itself but also by Silicon readout integrated circuits (ROIC) technology and components for cooling, if required.

Specific challenge

Access to 12'' silicon foundries is a key factor for recurrent cost optimization and because small nodes and 3D architectures will feature advanced ROIC, which are seen as key enablers not only for high-end IR detectors (all bands) but also for advanced thermal modules in the 2025-2030 timeframe. Moreover, this topic will require heavy budget allocation, which can be barely achieved at individual EU state level. Therefore the cost of access to advanced CMOS[20] node (65 nm and below) has to be shared at between the main EU players.

The proposals should mainly lead to the availability of an advanced EU ROIC supply chain compatible with various infrared detector technologies. It means:

- high resolution ROIC and compatible with 3D architecture to further enable advanced functions such as edge computing at sensor level;

[19] Detection, recognition and identification.
[20] Complementary Metal Oxide Semiconductor.

- an EU open silicon foundry and affordable price (thanks to collective specifications and orders).

To compete at the highest level of worldwide performance, the cooperation between the main EU infrared detectors suppliers is strictly required.

Complementarity should be ensured with past and current work funded through national programmes, the European defence agency framework, and other R&D programmes.

Scope

The proposals must address the development of the next generation of ROICs for Infrared detectors, including the EU supply chain. That next generation of ROIC will be based on an advanced Silicon technology (compatible with a 3D architecture) that can be used in various future cooled and uncooled IR detector architectures.

Targeted activities

The proposals must cover the following activities as referred in Article 10(3) of the EDF Regulation:

- activities aiming to create, underpin and improve knowledge, products and technologies, including disruptive technologies, which can achieve significant effects in the area of defence;
- studies, such as feasibility studies to explore the feasibility of new or improved technologies, products, processes, services and solutions.

These activities should be articulated as follows, without exceeding TRL 4:

(1) **from system requirements to ROIC technology specifications ("Improve knowledge")**: The targeted activities must in particular include, for both 2D and 3D ROICs, the collection and analysis of IR system integrators requirements; their translation into 2D and 3D building blocks, the prioritisation of these building blocks such as (and not exclusively) their coverage of future EU defence applications, an inventory of the Silicon nodes and IPs available in a selected EU foundry, and choice of the best one(s) to interface with different detector technologies (both cooled and uncooled) and be compatible with both 2D and 3D architectures;

(2) **identification and qualification of an advanced silicon node ("Improve knowledge")**: Furthermore for conventional 2D advanced ROICs they must include activities aiming at identifying and acquiring (a) new advanced silicon node(s) for future infrared detectors' read out circuits, such as interface definition and integration constraints with sensing blocks and packaging, both for cooled and uncooled detectors; definition of performance indicators to evaluate technical solutions versus the system integrators' requirements; test chip design(s)[21] for fabrication and test of 2D advanced

[21] Here, "Design » is a specific term in microelectronic to define the technological phase of building the sub-components of the ROIC to be tested. (It's therefore not to be understood as a design of a product).

functional blocks; characterisation, modelling and reliability activities on test chip specific patterns;

(3) **ROICs design [22], fabrication and functional test ("Improve knowledge" and "Studies")** This will prepare for necessary activities aiming at the electronic design, fabrication and functional test (first characterisations, excluding electro-optics) of (a) first high definition, large format, ultra-small pitch (≤7,5µm) 2D Read Out Circuit(s) with smart functions on this new CMOS platform(s); as well as preparatory studies to enable future ROIC functional routine tests at industrial level. When relevant some tests by system providers should be performed on the communication protocols based on the raw read out circuits;

(4) **preparatory work of 3D technology acquisition ("Improve knowledge")** on the selected node for 3D ROICs with increased functionalities at detector and pixel level will also be covered: exploration of 3D ROIC architectures allowing implementation of add-on functionality in a second layer, such as higher scene dynamics/reduced pixel pitches, in-situ image compression for large arrays/high frame rates, combination functions of passive/active imaging, event-based computing, in situ machine learning.

The implementation of this topic is expected to target TRL 4 for 2D advanced Read Out Circuits and to minimum TRL 2 (TRL 3 maximum) for 3D advanced Read Out Circuits.

Functional requirements

The proposed solutions should fulfil the following main high-level optronics system requirements:

- high resolution: increase in range and field of view, which translates at focal plane arrays into reduced pixel pitch and larger array imagers in the SWIR[23], eSWIR[24], MWIR[25] and LWIR[26] range, with formats ranging from 1 megapixels to 16 megapixels. (increasing interoperability and compatibility with cooled and uncooled detectors);
- high dynamics: higher scene dynamics for simpler, more compact and more tolerant to a wide range of operating scenarios optronics systems. This translates for example into multi-gain capability at pixel level, which will be a growing challenge as pixel pitch reduces;
- high speed: increase in image frame rate, which combined with the increase of the resolution, is requested for tracking and/or targeting fast-moving and possibly stealth threats. Advanced CMOS technologies are expected to provide significant gains in terms of operating frequency and thus data rates of IR ROIC;
- on-chip processing: towards systems-on-chip IR focal plane arrays with embedded, reconfigurable functionality depending on the application. The base idea is to make pixels

[22] *Idem.*
[23] Short wavelength infrared.
[24] Extended short wavelength infrared.
[25] Medium wavelength infrared.
[26] Long wavelength infrared.

smarter by integrating advanced computational functions at pixel level, through 3D stacked ROIC layers. Higher scene dynamics for reduced pixel pitches, *in situ* image compression for large arrays/high frame rates, combination functions of passive/active imaging, event-based computing are some examples of advanced integrated functions;

- significant gains in reducing power consumption for SWaP-C[27] detectors;
- ability to support dynamic windowing and tracking providing multiple windows of interest, and associated increased frame rate;
- fast event detection and decoding at pixel level.

Expected impact

- Driving factor for the development of tactical IR Optronics systems, reducing the time and cost development of Optronics systems.
- Ensure the dominance of future EU critical air combat and ground combat systems.
- Provide EU military forces with state-of-the-art IR detectors, ensuring the dominance of future EU critical platforms and armament systems.
- Improve DRI performances of IR sensors, especially for high-end platforms;
- Ease of use of smart IR modules.
- Develop an EU supply chain (especially for ROIC), contributing to the strategic autonomy of the EU.

2.4.2. Topic EDF-2021-SENS-R-RADAR: Advanced radar technologies

Nowadays, wide range of sensors, which are based on radar technologies, are applied during military operations. Radars are commonly used for supporting multi-domain operations: incl. air and air defence missions, as well as ground/maritime operations. Those technologies are crucial for space-/airborne-based, as well as ground-/maritime-based surveillance systems. Radar technologies are also used in various sub-systems of other purpose (*e.g.* engagement or logistics) military equipment.

Recent advances in digital signal processing and computing, radiofrequency (RF) and microelectronic technology have paved the way for the proliferation of active and passive radar technologies in a number of military applications. Management of the electromagnetic (EM) spectrum has also become more important year after year, and the usage of communications and internet of things (IoT) applications – which require more and more EM spectrum – generate increasing challenges during military operations. In addition, we must pay high attention to the strong technology push for the development of modular, smaller and state-of-the-art sensor applications, which are able to provide more functionality for the user in one device, are significantly less energy intensive, and can meet more operational needs.

[27] Size, Weight and Power - Cost.

Modern surveillance sensors have to comply with an unprecedented wide spread of operational requirements. A list follows hereby, which is not exhaustive:

- provide steady and reliable surveillance (detection, tracking, classification, identification) everywhere, at every time, at various environmental conditions – for every domain, with guaranteed low level of false alarm probability;
- addressing various types of standing installations and moving platforms (ground-based, shipborne, airborne, space borne), both manned and unmanned;
- covering broad spectrum of applications:
  - civilian, *e.g.* ATC [28] and weather forecast and monitoring, humanitarian (*e.g.* immigration, crisis management, like disasters, natural and caused by mankind), platforms' autonomy, space situational awareness, *etc*.;
  - military information superiority assurance: airspace, maritime and land traffic control; radio navigation; localization of our blue/red forces and resources; autonomous platforms; precision guided weapons; electronic warfare (EW).

Specific challenge

State-of-the-art military radar solutions must face challenges of modern battlefield, for instance:

- defence against very low RCS [29] targets (*e.g.* fast moving–fast manoeuvring, drones, hypersonic threats, stealth aircraft);
- detect long (strategic) range tactical ballistic missile (TBM) since boost phase, and wide spread of engagement means: rocket, artillery, RAM[30], loitering munitions;
- underground inspection, through the wall/vegetables surveillance;
- space surveillance and tracking: localization, classification and mitigation of space debris, enemy's space assets;
- able to operate in a limited EM spectrum resource (which today is a commodity) also complying with international and security regulations;
- to be open to operate as multi-role (radiolocation, communications, EW – electronic attack, non-cooperative target recognition, radar imaging, *etc*.) systems;
- to be resilient to harsh EM environmental conditions, with extensive jamming;
- go beyond the extraction of usual information to get intelligence from the measurements;
- use common/interoperable hardware (HW)/Software (SW) architecture and signal processing to support multi domain operation;

[28] Air traffic control.
[29] Radar cross-section.
[30] Rocket, artillery and mortar.

- cooperation and EM compatibility with other systems within a common recognized picture (battlefield situational awareness);
- coordinate and operate sensor management online/on the fly for joint improved performance.

Scope

Proposals should address the development of new concepts, technological blocks, sub-systems and/or systems in in order to realize a new class of sensors with remarkable sustainable characteristics in all domains (sea, land and air). They should include active and passive radars or radar sub-systems, as well as new system architectures of hardware building blocks and software modules designed to enable build up mission specific complex radar sensors and multi-functional radar solutions – eligibly in compliance with European Defence Agency's CapTech Radiofrequency Sensors Technologies' Overarching Strategic Research Agenda and its results (including TBB[31] in-depth analysis and their roadmaps), as well as previous EU funded activities.

These aimed achievements should be applicable in different kinds of active or passive radar systems (unification between different kinds of platforms desirable) and need to be able to support future military operations and to cope with new generation of unpredictable and unimaginable threats. For this reason, these activities should match with the following main abilities:

- the ability to provide integrated and modular system approach for military specific solutions;
- the ability to increase integration of more functions into one system;
- the ability to increase the proliferation of radar-based sensor applications for wide scale of military operations;
- the ability to enable versatile deployment for the large spectrum of military operations;
- the ability to enable high operational availability (*e.g.* by fault tolerance techniques and relative technologies adoption);
- the ability to apply radar either as a main element or sub-system of one complex equipment regardless of the operational context;
- the ability to use a radar as a node in a more complex network;
- the ability to primarily enable efficient software (HW desired as well) upgrades during life cycle;
- the ability to provide new system test and evaluation (T&E) methods based on RF and/or digital scenario emulators/simulators.

[31] Technological building blocks.

Targeted activities

The proposals must cover the following activities as referred in Article 10(3) of the EDF Regulation, not excluding downstream activities eligible for research actions if deemed useful to reach the objectives:

- activities aiming to create, underpin and improve knowledge, products and technologies, including disruptive technologies, which can achieve significant effects in the area of defence;
- activities aiming to increase interoperability and resilience, including secured production and exchange of data, to master critical defence technologies, to strengthen the security of supply or to enable the effective exploitation of results for defence products and technologies;
- studies, such as feasibility studies to explore the feasibility of new or improved technologies, products, processes, services and solutions;
- the design of a defence product, tangible or intangible component or technology as well as the definition of the technical specifications on which such design has been developed which may include partial tests for risk reduction in an industrial or representative environment.

In particular, the proposals must address the following activities:

(1) activities aiming to create, underpin and improve knowledge and technologies, including disruptive technologies, which can achieve significant effects in the area of defence:
   - definition and analysis of technology trends and implementation opportunities (desired final parameters and functionalities in particular) of state-of-the-art and future technologies such as: *e.g.* RFSOC[32] (SIP[33]), compressive sensing for imaging or/and MTI[34], MIMO[35] mode, polarimetry, machine learning for supporting radar signal processing, recognition and classification;
   - deep analysis of theoretical basis for a scope of the proposed project;

(2) activities aiming to increase interoperability and resilience, including secured production and exchange of data, to master critical defence technologies, to strengthen the security of supply or to enable the effective exploitation of results for defence products and technologies:
   - operational requirements and military usage scenarios, identification of operational benefits and sizing requirements of technological breakthroughs;
   - definition of security, cyber and interoperability needs for future challenges;

[32] Radiofrequency system on chip.
[33] System in package.
[34] Multi target indication.
[35] Multiple-input multiple-output.

- basis for common standards definition;

(3) preliminary/feasibility activities and studies to explore the feasibility of new or improved technologies, products, processes, services and solutions:

- definition and analysis of behaviour and detectability of targets;
- definition of EW functionalities and technology in radar and communication band;
- definition of cognitive radar, digital radar and waveforms for increased deployment versatility;
- analysis regarding the use of software defined radar in order to improve the flexibility of future solutions;
- definition of CONOPS (concept of operations);

(4) design of a tangible or intangible defence component/sub-system, system or technology as well as the definition of the technical specifications on which such design has been developed which may include partial tests for risk reduction in representative environment:

- top level sensors specifications and high level design (including adaptive digital beam forming, transmitted power, bandwidth, spectral purity, power consumption, production cost…);
- definition of the functional and physical architectures of the transceiver building block (interfaces, partitioning, type of semiconductor process, packaging…);
- definition and development of waveforms/data exchange (standardization);
- development of operational capabilities based on distributed, multi-static configuration (incl. active/passive (both collaborative and non-cooperative illuminators)/mixed mode), or new application methods;
- development of integrated solutions for time synchronization and multi sensor data fusion (*e.g.* Concerning time synchronization and platforms geo-localization, especially in GNSS denied zone), data storage and system resource management;
- development of integrated solutions for microwave high-power generation, for robust and highly digitised receivers, for radar signal generation and its distribution, for adaptive distributed beamforming, for multi-functional array transmitters; a new paradigm by the development of the so-called "chiplet" approach – an integrated circuit block that is specifically designed to work with other similar chiplets to form larger chips that are more complex. This approach can also be used for SOC (*i.e.* with integration on the same semiconductor substrate) or SIP (*i.e.* with heterogeneous integration);
- reduction of PCBs [36] by using hybrid packaging techniques for different semiconductor technologies integration;

[36] Printed circuit boards.

- definition and development of security, cyber and interoperability needs for future challenges;
- test case as a basis for demonstration, simulation and prototyping;
- integrated and aligned operation demonstration;
- (cognitive and/or machine learning-based) sensor data fusion and complex object/target classification;
- risk mitigation;
- presentation of results and execution of a demonstration through one or more test scenarios.

In addition, proposals could cover both HW and SW solutions, of various integration scale (materials, components, sub-systems and systems) in the representative areas as follows:

- detection, tracking and recognition/identification (including SAR[37]/ISAR[38]/3D ISAR – passive and active imaging techniques) of new and challenging targets, such as made according to stealth philosophy, of low radar cross section, small (drones), fast moving and manoeuvrable (*e.g.* hypersonic missiles, UAVs[39], *etc*.);
- contribution to kill assessment functionality;
- intelligent radar decoys;
- intelligent and cognitive resource management;
- multi-platform, multi-static and multi-functional RF systems for air defence and battlefield (in all domains: air and space, land and maritime) surveillance;
- specific radar applications, such as *e.g.* navigational equipment (for airspace management, as well as various platforms situational awareness), missile/artillery munitions radar homing, battlefield radars, ground and vegetation penetrating radars, through-the-wall radars, dual polarization weather radar, *etc*., supported by disruptive technologies for increased system capabilities;
- electronic warfare capabilities (both defensive and offensive, *e.g.* low probability of intercept, effective jamming suppression, jamming of netted sensors, *etc*.);
- system maintenance concept and high operational availability (*e.g.* by health and usage monitoring system (HUMS) and self-healing techniques);
- design that enables continuous upgrades during the life of the system (*e.g.* using new software defined radar (SDR) technology);
- development of system T&E methods.

[37] Synthetic aperture radar.
[38] Inverse synthetic aperture radar.
[39] Unmanned aerial vehicles.

A preliminary plan (roadmap) for the potential utilization by subsequent development phases should also be presented, with a special focus on the capability needs of Member States, as well as expected improvements in comparison with existing solutions.

Functional requirements

Requirements are based on the potential development of a multi-platform RF system which will be able to support directly military operations based on the specific challenges described earlier. The proposals should therefore meet the following functional requirements:

- to demonstrate better understanding of the new challenges for future operational and tactical environment requirements;
- to provide increased and more operation capability in detection of new challenging targets, objects and (manned-unmanned) swarms, moreover wide configuration opportunity for mission specific tailored applications;
- to provide solutions for multi-mission applications (maritime, land and air);
- to provide solutions compatible with modular and scalable architectures in order to fit different further applications;
- to provide solutions compatible with multi-static and distributed systems;
- to provide designs with low-cost production;
- to provide better performance parameters, especially measurement accuracy (range, azimuth, height) as well as low SWaP (size, weight and power) for demanding applications (*e.g.* airborne);
- to decrease significantly the sensor-to-effector lead time;
- to enhance ECM[40] (against radar and communication signal) capabilities against new generation threats;
- to build integrated complex RF applications for one or more mission specific function, like digital beam forming and RF sampling and digitalization of signals at carrier frequencies;
- to provide solutions compatible with software defined methodology for the implementation of sensor functions;
- to push the technological solution scope by investigating dedicated power and mixed-signal technologies;
- to build on high-power front-end components (as developed through the call “materials and components \ advanced radio frequency components”;
- to provide deep integration in common configuration and sensor fusion;
- to apply/allow to apply recent achievements of big data, artificial intelligence, machine learning and software algorithm techniques in the signal processing, in the flexible operation support and in the automatized decision-making process;

[40] Electronic countermeasures.

- to contribute to increasing force protection, resilience, timely decision-making through modern and intuitive user interfaces that support operators in all their operational, technical and training needs;
- to increase sensors mobility and sensor reliability through innovative solutions for thermal management and reliable power supplies development;
- to provide deployment and interoperability with wide range of military systems, effectors.

Expected impact

(1) From a technical point of view:

- increased application capability for detection, identification of different kind of threats, including new types of increased velocity and hypersonic targets, missiles and field objects;
- wide range of application opportunities for EU military operations;
- improved critical awareness as deterrent;
- increased operation capability in harsh EW environment and under active electronic countermeasures;
- increased mission specific solutions with the opportunity of multi-mission and multi-function application capability;
- competitive services with embedded solutions of new approaches and applications of future disruptive technologies, such as artificial intelligence, advanced new materials and structures, additive manufacturing in electronics and antennas or nano-technology, neuro science-based HMIS.

(2) From a policy point of view:

- development of critical enablers for CSDP operations and EU Battlegroup missions;
- enhanced force protection;
- increased military capability in joint military missions;
- improved situational awareness, resilience and security of EU military operations;
- improvement of one of the key European defence industrial capabilities;
- strengthening the EU's strategic autonomy in the production of military related RF applications;
- reinforcement of interoperability between EU Member States' armed forces;
- reducing the cost of European military missions;
- reducing the impact of the EM spectrum usage.

2.5. Call EDF-2021-CYBER-R: Cyber threat intelligence and improved cyber operational capabilities

Proposals are invited against the following topic:

- **EDF-2021-CYBER-R-CDAI:** Improving cyber defence and incident management with artificial intelligence.

Budget

The Union is considering a contribution of up to EUR 13 500 000 to support proposals addressing the abovementioned topic and its associated specific challenge, scope, targeted activities and functional requirements.

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

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

2.5.1. Topic EDF-2021-CYBER-R-CDAI: Improving cyber defence and incident management with artificial intelligence

The ability to detect and respond to security incidents suffers from several challenges, including: the ever increasing amount of data that needs to be analysed in order to detect and fully understand security incidents; the number of false alarms generated resulting in, for instance, erroneous prioritisation and alarm fatigue amongst operators and analysts; lack of (human) resources to sufficiently analyse all potentially malicious activity; the decreasing effectiveness of traditional defence measures based on known set of rules (*e.g. a priori* known signatures and/or network traffic profiles) due to the increase of encrypted network traffic and their inadequacy against advanced persistent threats and zero-day attacks (including malware that exploits unknown vulnerabilities, targeted phishing attacks, low-rate data exfiltration, abnormal user behaviour, *etc*.); choosing appropriate measures in response to attacks in a timely manner, when the scope is uncertain and the situation develops faster than a human being may follow without advanced decision-making support, and while the compromise potentially have or will extend over weeks, months or years.

The use of Artificial Intelligence (AI)[41] seems promising in order to address many of these challenges – and AI has recently shown great results in areas such as playing strategic games and analysing text.

This call seeks proposals that help increase the level of automation in incident management and cyber defence activities through the use AI. In this setting, the engagement of state-of-the-art AI methods should be used to automate incident management and cyber defence activities, including incident detection and response, carried out by security operation centres (SOCs), and cyber defence teams (or similar entities) when they detect and analyse events and determine what actions to take.

[41] *e.g.* machine learning, deep learning, decision trees, statistical outliers, probabilistic networks, genetic algorithms, reinforcement learning, situation calculus, ontologies, symbolic reasoning, *etc*.

Modern SOCs are sometimes equipped with security orchestration, automation and response (SOAR) capabilities that allows human operators to respond to attacks with predefined "playbooks" designed to mitigate ongoing attacks, *e.g.* by disabling user accounts or reconfigure firewalls, where AI-based solutions seem applicable.

AI can, for instance, be used to complement rule-based detection methods (*e.g.* through deep learning), to enhance alarms from detection systems using threat intelligence feeds, extract actionable intelligence from the enormous amount of monitoring data and events, correlate alarms with other information to identify attack patterns, automatically respond to events based on the analysis, and recommend actions to human operators. Recent studies unveil that more than two-thirds of the organisations included in the studies acknowledge that they are not able to respond to critical threats without AI.

Specific challenge

Creating an AI-based solution that automates larger parts of incident management and cyber defence processes involves several technical challenges. These include (among others): the selection and pre-processing of appropriate data sources; creating and applying models and techniques for analysing the output of sensors to assess if an attack may be happening, including selection and tuning of algorithms and parameters; mapping ongoing attacks to known threats (*e.g.* using threat intelligence); assessing if the consequences of implementing a particular response outweigh the risks associated with not doing so; and creation/selection of appropriate datasets for training and testing the models. Moreover, transparency and configurability are key requirements, especially in the military domain, which is lacking for most commercial Security Information and Event Management platforms (SIEMs).

While AI-based solutions may be required to address these challenges in this ecosystem, incorporating AI also introduces a new set of technical and non-technical challenges. Questions addressing technical challenges: At which point should an alarm be raised and when should it be elevated? How can AI reason about trust with respect to the use of external information (*e.g.* threat intelligence)? How can the possible consequences of a cyber-attack, and the consequences of implementing different mitigating means, be assessed before and during response, both in real-time, near real-time/short term or as part of a medium or long term defensive strategy? Many incidents will (at some level) require human interaction and human decision-making – how does an AI-based system communicate the results and the underlying explanation and reasoning leading to the result? Non-technical challenges include: Which decision rights and processes can, and should, be delegated to an AI-based system and which should remain manual? How should AI be utilised at strategic, tactical and more technical levels? What is the difference between communication at a technical, tactical, operational and strategic/political level? How can humans work together with AI-based systems at the different levels? Military systems increasingly use, and depend on, the private sector and civilian infrastructure – how does incident response differ between military and civilian sectors and what are the challenges in a combined military/civilian setting? What are the implications for AI?

Scope

Addressing the identified challenges will require inter- and multi-disciplinary approaches, where teams conduct work of both a technical and a non-technical nature. Analysis of technical, tactical, operational, strategic and political considerations are required. On a technical level, proposals should provide proof-of-concept solutions for AI-based incident management and cyber defence, including detection, mitigation and response. Capable intrusion detection systems (IDS) could form a starting point for proposals. However, proposals must not seek to further the analysis capabilities of IDS alone, but in the context of an automated or semi-automated system for handling incidents.

In additional to purely technical solutions, processes and actors of selected enterprises may need to be mapped, modelled and understood to ensure fit-for-purpose solutions and answer questions of a more conceptual nature. Proposals are further expected to consider the interaction between human operators, analysts and decision makers and the automated or semi-automated incident management and response system.

A suitable methodology for building contextual understanding is expected through case studies of selected processes, incidents and cyber-attacks of selected enterprises, and case studies of successful detection approaches and resilience oriented success stories where technical and non-technical challenges can be studied and addressed at different levels. For the development of technical proof-of-concept prototypes, an appropriate development approach, which includes user and stakeholder involvement, should be leveraged.

Targeted activities

The proposals must cover the following activities as referred in Article 10(3) of the EDF Regulation:

- activities aiming to create, underpin and improve knowledge, products and technologies, including disruptive technologies, which can achieve significant effects in the area of defence;
- activities aiming to increase interoperability and resilience, including secured production and exchange of data, to master critical defence technologies, to strengthen the security of supply or to enable the effective exploitation of results for defence products and technologies;
- studies, such as feasibility studies to explore the feasibility of new or improved technologies, products, processes, services and solutions
- design of defence products, tangible or intangible component or technology as well as the definition of the technical specifications on which such design has been developed which may include partial tests for risk reduction in an industrial or representative environment.

All proposed activities ultimately support the creation of fit-for-purpose proof-of-concept prototypes of an automated or semi-automated incident management and cyber defence system, for select phases in the incident management cycle including detection and response. The prototypes may support human operators, analysts and decision-makers at all levels (technical, tactical, operational, strategic and political) and are expected to contribute to

enhanced cyber situational awareness, increased military infrastructure resilience and improved protection against advanced cyber threats.

The activities are sorted into three types of tasks:

1. Enhancing contextual knowledge of the enterprises, processes and decision-making where AI should be utilised;
2. Developing AI-based techniques supporting specific human operator/analyst tasks;
3. Exploring and developing AI as a decision-maker given limited authority in incident management and cyber defence.

Feasibility studies drawing upon real-world scenarios should be utilised to ensure that developed proof-of-concepts and techniques are fit-for-purpose. It may also be necessary to create reference systems and appropriate tests cases to generate training data and evaluate the efficacy of different solutions, both with and without human operators interacting with the system.

The proposals[42] must include at least one activity from task 1 and one activity from task 2 and must be coherent with the defined scope as described above.

1. Enhancing contextual knowledge of the enterprises, processes and decision-making where AI should be utilised

   1.1. Knowledge building through analysis of real-life situations, use cases and incidents, in order to sufficiently understand and model the enterprise processes and decision-making processes that AI-based incident management and cyber defence systems will interact with. This includes understanding the relevant actors, their enterprises and business/missions, and the threat environment they operate in.

   Proposals may include processes and work flows involving human operators, analysts and decision makers at all levels. Proposals may also cover elements such as information requirements, dealing with uncertainty, strategic objectives, mission objectives, the role of ICT, risk analysis, risk appetite, incident and crisis communication to different stakeholders, *etc*.

   1.2. Exploring the boundaries for AI-based autonomous or semi-autonomous response. The playbooks of many SOCs and similar entities describe how to respond to given attacks. However, in depth understanding of the broader context is necessary in order to avoid inappropriate measures. To take into account the broader context in order to avoid inappropriate measures at least the following questions may be addressed: Can such playbooks be automated and can AI reasoning capabilities automate such intuition, experience and contextual understanding? When most machine learning and deep learning algorithms require a vast amount of data to learn from, which will not be available for incident response, can one-shot/few-shot learning (*e.g.* human-style learning) be utilised in this setting to learn how operators respond to incidents? Can

[42] Proposals are not expected to include all listed tasks.

symbolic approaches work in conjunction with machine learning (*e.g.* neuro-symbolic AI) to automate playbooks?

2. Developing AI-based techniques supporting specific human operator/analyst tasks

   2.1. Creation of AI-based techniques for detecting and understanding adversarial activity. This may include analysing and triaging alarms, conducting forensics, utilising external information with varying levels of trust (*e.g.* threat intelligence), leveraging behavioural analytics, performing kill-chain detection and analysis, assessing potential attacker intentions, monitoring applications and communication activities, analysing malware, etc. The techniques may be intended for both real-time and non-real-time detection and analysis, involve multi-disciplinary approaches, use data from endpoints, networks and the cloud, and leverage distributed computing and data processing for real-time scalability.

   2.2. Creation of AI-based techniques for building knowledge about own protected ICT systems (*e.g.* a "cyber record" with current and historical information). This must include collecting, linking and fusing different kinds of information about the system hardware, software, and the relationship between them. Information that may be collected is, for instance, architecture and configuration data, hardware location and specifications, installed applications, network information, services, protocols in use, connected peripheral devices, *etc*. A variety of sources may be leveraged for acquiring information, including hardware and software configuration management systems, documentation, vulnerability scanners, SIEMs, asset discovery tools, *etc.*, and techniques such as reverse engineering may be utilised.

   2.3. Creation of AI-based techniques for analysing enterprise systems to appraise the value of assets and the potential consequences of different responses (*e.g.* configuration changes). This must include both static values manually assigned or derived from fixed factors, and dynamic values that must be seen in relation to ongoing and changing business operation or military missions.

   2.4. Creation of explainable AI-based techniques. Many of the most promising machine learning systems are not considered to be "intelligible" or "explainable", which has resulted in a sub-field coined explainable AI (XAI). This task should address how XAI can be utilised to explain detection, analysis and responses at different levels to different actors? Can, for instance, machine learning (*e.g.* deep learning) be combined with more traditional symbolic AI to make the analysis transparent?

3. Exploring and developing AI as a decision-enabler given limited authority in incident management and cyber defence

   3.1. Creation of AI-based information collection and storage systems that dynamically adapts its collection and storage strategy to the situation as continuously analysed and perceived by the system. This includes what is collected, where it is collected and the granularity (*e.g.* increasing the level of detail of collected information, such as full packet capture, after an initial compromise is detected). As it is not feasible to collect

everything and everywhere, such dynamic big data analytics and data lake systems could help the issue of insufficient data due to limited data collection.

3.2. Creation of AI-based decision systems which are risk and impact aware. They should be able to analyse and understand the impact of security incidents on desired mission performance, identify associated risks, generate different response options to maintain requisite cyber resilience and mission assurance, and potentially select and execute a response option if permitted. The analysis of impact, risks, different response options and potential execution should be explainable.

Functional requirements

The proposal must address:

- at least one framework for mixed AI-human cyber defence and incident response suitable for either military or civilian contexts, or both;
- at least one proof-of-concept prototype of an automated or semi-automated incident management system, for select phases in the incident management cycle including detection and response.

Requirements are set across the following categories:

- architecture and design;
- integration with existing systems;
- utilization of AI/ML for certain tasks;
- reasoning, learning and validation.

Architecture and design:

- the proposal should include an architecture that is open, modular, scalable, resilient and highly available;
- the proposal could include graphical and programmable interfaces to communicate with both operators and other programs;
- the proposal could include secure cooperative training and sharing of models between different organisational units and nations, *e.g.* through federated learning.

Integration with existing systems:

- proof-of-concept prototypes should be able to collect telemetries or raw data from existing sources (*e.g.* sensors systems), including information such as endpoint metrics and logs, network traffic information (*e.g.* Netflow), and events and logs from both security appliances and application servers;
- it is desirable for proof-of-concept prototypes to interact with, and leverage, existing rule-based detection and classification solutions for coordinated utilisation of both AI and non-AI techniques.

Utilization of AI/ML for certain tasks:

- proof-of-concept prototypes should engage AI/ML in order to improve incident detection rates (*e.g.* accuracy and recall), compared with existing rule-based solutions;
- proof-of-concept prototypes should engage AI/ML to automatically propose and potentially effectuate mitigating actions.

Reasoning, learning and validation:

- proof-of-concept prototypes should be able to explain their reasoning and decision making to human operators. It is desirable that algorithms and models are transparent, documented and configurable by the user;
- proof-of-concept prototypes should be possible to train and configure with information that is readily available or straightforward to produce in contemporary enterprises;
- proof-of-concept prototypes must be validated in a relevant environment (*e.g.* reference system) when exposed to relevant test cases (*e.g.* contemporary network attacks).

Expected impact

- Knowledge on the use case(s) for automated and semi-automated incident response systems, including their practical feasibility and usefulness, limitations, integration into manual processes and interaction with human operators.
- Proof-of-concept for AI-based capabilities for incident detection, analysis and response of selected attacks and scenarios.
- Advanced preparedness of cyber defence operators and improved cyber operational capability, which contributes to EU cyber defence posture.

2.6. Call EDF-2021-CYBER-D: Improved capacity for cyber training and exercises

Proposals are invited against the following topic:

- **EDF-2021-CYBER-D-IECTE:** Improved efficiency of cyber trainings and exercises

Budget

The Union is considering a contribution of up to EUR 20 000 000 to support proposals addressing the abovementioned topic and its associated specific challenge, scope, targeted activities and functional requirements.

Up to one action may be funded under this call.

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

2.6.1. Topic EDF-2021-CYBER-D-IECTE: Improved efficiency of cyber trainings and exercises

Specific challenge

Personnel development is one of the key requirements for effective cyber defence. Extensive trainings and exercises constitute the best means to enhance and validate the skills of the cyber defence workforce. For this, Member States have invested in establishing cyber ranges that provide controlled artificial environments where, among others, malicious activities can be simulated without negative impact on live systems in an organization. However, the existing cyber ranges can be developed further to achieve their full personnel development potential. In turn, it supports cyber operators improving their skillset and benefits military commanders in understanding cyber as a cross-domain challenge. This includes addressing threats and opportunities driven from the emerging disruptive technologies.

The proposals are expected to address the following challenges:

- first, the maturity level of user simulation running on cyber ranges is low. The user simulation is often limited to traffic generators and tools for testing user interfaces for a well-defined purpose. User simulation, which leaves a non-detectable footprint and produces logs while being indistinguishable from the real human users', is needed for providing more meaningful, realistic and life-like scenarios for exercises and training sessions. Additionally, scenarios that rely on the actions of simulated users, *e.g.* because of phishing emails, require a solution that gives the training or exercise organizer control over the user simulation to make sure simulated users act in accordance to the scenario;
- second, cyber ranges lack capabilities to assess and reflect the decision-making process of cyber operators during an exercise or training. Current systems fail to provide insight to the particular actions cyber operators perform to achieve the objectives. This includes unanswered questions such as which tools and commands were used and options selected in the graphical interface, who was communicated with (both online and in the war-room), what was searched online (and whether that was useful). This presents additional challenges as systematic monitoring and assessment of skill gaps is not possible, especially for more complex exercises. However, automated performance assessment and analysis of the participants allows the training and exercise instructors to monitor either on individual or team level their performance in more detail;
- third, scenarios involving user-simulation and systems enabling analysis and assessment of the decision-making process of cyber operators should be accessible and interoperable for different cyber ranges. This can be enabled through scenario development language. Besides potential cost-efficiency, it also improves and upgrades the scenarios over time based on feedback by many users. Hence, simulated users, scoring system and the analysis of the operators' performance can be accordingly elevated, training and exercises therefore continuously improved;
- fourth, so far, many cyber ranges focus only on one domain and its functionalities, but the impact of cyber-attacks must be considered as a cross-domain challenge. Therefore, a multi-domain cyber range simulation must support and simulate land, air, sea and space

domains. This includes, for example, military systems (*e.g.* battle management systems), radio and operational technology. Especially the integration of the electromagnetic spectrum (EMS) and the common understanding of cyber and EMS should be a key factor of future cyber ranges. The challenge is to support a highly realistic simulation of multiple domains, the interconnection of systems and to assess the impact of the inter-dependencies between those systems. Such simulations would support the training and evaluation of multi-domain common operating pictures and its operations as well as development and testing of new military approaches and doctrines to cyber/EMS threats;

- last, conducting large-scale cyber exercises or simulating real-life modern ICT environment requires unique and complex set of capabilities and infrastructure (such as specialized hardware to simulate cellular networks, industrial controllers and other parts of critical infrastructure). The most practical way to create such complex environments is through cooperation among Member States and federating cyber range infrastructure and exercise content. Such approach requires development of common standards, protocols, and software solutions to allow federated scoring and situational awareness throughout the federated environment.

Scope

The objective of this topic is to create a toolset that allows significantly increased efficiency in the cyber trainings and exercises process while also enhancing cyber ranges interoperability and cost-efficiency, taking into account challenges described.

To develop a technological demonstrator modules that can be easily configured and interfaced to existing systems used to conduct cyber trainings and exercises. Integration of the technologies must be demonstrated within TRL 4-8, but specific TRL may wary depending on the work package.

Simulated users

Development of agents capable of using common software applications in a similar manner to human users. Actions in scope for the user simulation is benign use of common software applications (*e.g.* word processors, web browsers, file management applications, and email clients). The solution is able to replay sequences such actions obtained from the automated performance analysis when human operators has used systems and allows custom behaviours to sequences of such actions to be crafted. Furthermore, the solution also allows custom modifications of action sequences obtained from the automated performance analysis, *e.g.* to modify a sequence of actions to create an alternative scenario. Simulated users be used to, among other things, simulate social engineering incidents (*e.g.* phishing), the generation of system logs, and the generation of network logs. The footprint of the simulated users is indistinguishable from those of real users in logs and must be visible in graphical user interfaces.

Automated performance analysis

Development of a system capable of collecting data about the cyber operators' activities during trainings and exercises, and automatically analysing tasks of low to medium complexity while also providing supporting data and insight to evaluate advanced situations

which are often difficult to fully assess through automated techniques. This should be based on combining already well-researched and documented methods (*e.g.* application programming interfaces (APIs)), and big data analysis, image analysis and neural language processing to collect and analyse cyber operator's behaviour during training and an exercise.

Scenario development language

Scenario development language enables scenario sharing with other cyber ranges and ensures interoperability between different cyber ranges. While the cyber ranges are interoperable regarding more common activities (training, exercises, *etc*.) and more complex scenarios can be implemented raising the overall preparedness of cyber operators utilizing the capabilities. The language itself should be described based on research of existing cloud and virtualization topologies and should be extended with specific components (simulation, scoring, federation, *etc*. attributes) that are needed in the cyber range environments.

Multi-domain simulations

Development of enhanced multi-domain cyber range simulations for at least 2 domains (*e.g.* land, sea and/or space) and the standards and interfaces to interconnect relevant systems and environments (*e.g.* battle management systems, EMS or other systems) in order to allow simulation of realistic joint cross-domain scenarios and situational awareness.

Situational awareness and scoring

The activities include developing standards and protocols for federated scoring system, exchange of situational awareness information, including federated cyber range operation.

Targeted activities

The proposals must cover the following activities as referred in Article 10(3) of the EDF Regulation, not excluding upstream or downstream activities eligible for development actions if deemed useful to reach the objectives:

- studies, such as feasibility studies to explore the feasibility of new or improved technologies, products, processes, services and solutions;
- the design of a defence product, tangible or intangible component or technology as well as the definition of the technical specifications on which such design has been developed which may include partial tests for risk reduction in an industrial or representative environment;
- the development of a model of a defence product, tangible or intangible component or technology, which can demonstrate the element's performance in an operational environment (system prototype);
- the testing of product, tangible or intangible component or technology.

The proposals must address in particular the following tasks:

Simulated users

- study the methods and technologies to develop simulated user;

- develop a prototype for simulated user capable of using common software applications while producing realistic logs and footprints in the machines;
- develop a method for converting recorded behavioural data of cyber operators that can be used in the user simulation;
- proof of concept testing and validation of the proposed toolset to present that the user simulation produces a footprint similar to normal users when it is applied.

Automated performance analysis

- study the methods and technologies that provide information about the decision-making process during a training or exercises (*i.e.* consoles, graphical interfaces (including videos from environment), network traffic, audio between team members));
- study the technologies to gather, store and process information produced during a training or exercise;
- design methodology to correlate cyber-attacks data and collected cyber operators behavioural data, and the ways to improve the individual and collective performance of cyber operators. The methodology should also provide feedback loop for exercise designers to improve the learning effect of the exercises;
- design methods to ensure the integrity of the automated analysis process and/or consider classification of military environments;
- develop a prototype for the automated analysis that includes at least logging, data parsing and performance evaluation functionalities;
- proof of concept testing and validation of the proposed toolset.

Scenario development language

- study existing cloud and virtualization topologies, including defining data format to define a common scenario language that can be used by different cyber ranges;
- develop an extendable scenario development language in coherence with the other capabilities described in this call;
- proof of concept testing and validation of the scenario development language on an existing cyber range.

Multi-domain simulations

- develop standards and interfaces for interconnecting multi-domain cyber ranges (*e.g.* land, air, sea and space) for cyber trainings and exercises;
- develop multi-domain scenarios for capacity building;
- proof of concept testing and validation of the proposed toolset.

Situational awareness and scoring

- study the existing technology solutions used by Member States for cyber ranges' situational awareness and implement the solution in federated environment;

- design common standards for cyber ranges' situational awareness.

Functional requirements

General

- the methods and technologies proposed and developed can be implemented in most existing cyber range environments.

Simulated users

- the simulated users must be able to perform common actions in commonly used enterprise software (*e.g.* word processors, web browsers, file management applications, and email clients);
- the simulated users must produce logs in the machines that, using commonly used log analysis tools, cannot be distinguished from the logs produced by humans performing the same actions;
- the actions performed by the simulated users must be possible to schedule using recorded actions of human operators, with a crafted specification detailing actions, and through the combination of recorded actions and crafted specifications.

Automated performance analysis

- cyber operators in the training or exercise environment are identified and the information processed is linked to specific operators, which allows monitoring and automatic analysis of cyber operators' activity on individual and team level;
- the analysis of the cyber operators' behaviour must be done in near-real time, and there must be an option to customize the set of-rules and parameters depending on the training or exercise;
- reporting of the analysis of the cyber operators' activity should be displayed according to the timeline of the exercise or training;
- both cloud computing and on-premise solutions must be available for the cyber range operators depending on the classification level of the environment.

Scenario development language

- scenario development language should take into account previously conducted related research and development, *i.e.* should have a functionality similar to OASIS Topology as well as Orchestration Specification for Cloud Applications (TOSCA) version 1.3 [43], OpenStack or other cloud architecture solutions;
- scenario development language must be machine and human-readable, use English syntax and be based on textual language (also have graphical representation), be scalable and extendable, enable using regular expressions and analysing capabilities, enable commenting the content;

[43] *TOSCA Simple Profile in YAML Version 1.3.* https://docs.oasis-open.org/tosca/TOSCA-Simple-Profile-YAML/v1.3/os/TOSCA-Simple-Profile-YAML-v1.3-os.pdf.

- scenario development language should at minimum support definitions such as network, virtual machines, external component configuration, and post-deployment actions;
- scenario development language should allow post-deployment actions, *e.g.* verification of the deployed system against the planned description;
- the language for post-deployment actions (*e.g.* simulated users and attacks) should provide control over the timing of events and enable the creation of dynamic plans where actions depend on the current state of the cyber range environment and the outcome of previous actions;
- scenario development language should enable a common analysis of indicators of compromise (IOC) and malicious artefacts (operational level).

Multi-domain simulations

- the proposed solutions on cyber range should provide simulations for at least two domains;
- the simulations should not only include simulations on the network layer and above (Open Systems Interconnection, (OSI) model layer 3+), but also include data link and physical layers (OSI model layer 1-2).

Situational awareness

- situational awareness protocols and solution must be sufficient for tracking typical large scale cyber exercise needs[44];
- existing software solutions must be taken into account when developing standards, protocols, and solutions to ease integration and interoperability.

Expected impact

- Advanced preparedness of cyber defence operators and the capacity and interoperability of cyber ranges, which contributes cost-efficiently to EU cyber defence posture.
- The methods and tools provided will offer a better understanding of the decision-making process, both on the individual and team levels. Individuals and teams can have *post mortums* to gather lessons identified from the training or exercise. The results must also be comparable between several trainings and exercises. A strong data-based approach supports organizers in performing analytic evaluation to improve the quality of an exercise, evaluate its impact on learners compare the effectiveness of different approaches, and refine and enrich training scenarios.
- Based on the methods and tools developed for understanding the operator's decision-making process, a framework for modelling simulated users can be developed. This capability reduces the need for human interventions but increases the quality of the cyber trainings and exercises. Realistic normal system usage also serves as background traffic in intrusion detection tests, thereby supporting the development of tools for cyber situational awareness.

[44] A large scale cyber exercise can be understood for instance as an exercise that has more than 100 participants and 50 observers.

- The ability to facilitate cyber trainings and exercises in a federated environment will increase cooperation among member states, efficiency of organizing large-scale exercises, and complexity that can be achieved realistically in such exercises. Thus, improving the overall effectiveness of cyber trainings.
- These benefits will ultimately result in lower cost and larger number of successful trainings. Better-organized exercises will help to gain skill improvements quicker and with less hours of training.

2.7. Call EDF-2021-SPACE-D: Resilient space-based PNT and SATCOM

This call aims at improving space-based PNT resilience in contested environments through the mapping and analysis of threats. It will complement the on-going EDIDP project on Galileo PRS receivers and contribute to reinforce Galileo as a credible European solution for defence applications.

This call aims also at accompanying the development of European technologies and products for interoperable and resilient military satellite communications.

Proposals are invited against any of the following topics:

- **EDF-2021-SPACE-D-SGNS:** Space and ground-based NAVWAR surveillance;
- **EDF-2021-SPACE-D-EPW:** European protected waveform and accompanying technologies for resilient satellite communications against jamming.

Budget

The Union is considering a contribution of up to EUR 50 000 000 to support proposals addressing any of the abovementioned topics and their associated specific challenge, scope, targeted activities and functional 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.

2.7.1. Topic EDF-2021-SPACE-D-SGNS: Space and ground-based NAVWAR surveillance

Specific challenge

Navigation Warfare (NAVWAR) concept appeared in PNT[45] landscape more than twenty years ago. During those past decades, the PNT defence community mainly focused on acquisition and toughening GNSS (Global Satellite Navigation Satellite System) user segment, improving inertial sensors, and exploring alternate PNT capabilities (*e.g.* vision-based navigation).

[45] Positioning, Navigation and Timing.

Further work is nevertheless required to achieve PNT superiority in joint operations/missions. Indeed, NAVWAR entails more than resilient GNSS-based equipment or GNSS-free sensors. It also consists in knowing and dealing with the threat (*e.g.* on performing a spectrum and spatial surveillance). Some R&T initiatives allowed identifying some promising tools and technologies, but PNT sensors in use today mainly supports resiliency aspects of NAVWAR, and so do not fully provide a full-spectrum capability.

PNT sensors need to be resilient, but also to deliver information for NAVWAR surveillance and NAVWAR offensive measures. Galileo PRS[46] receivers themselves should contribute to the full-spectrum NAVWAR capability, becoming part of a NAVWAR sensor network, leveraged by associated C2 systems. Therefore for the targeted NAVWAR capability, a wide range of sensors including mobile applications (*e.g.* smart architectures, hand-held PRS receivers) and space-based surveillance needs to be available, in conjunction with Galileo PRS signal and service, in order to support a comprehensive NAVWAR situational awareness picture and NAVWAR offensive measures.

To face this challenge and preserve Europe sovereignty, this call topic aims at building an EU NAVWAR capability gathering efforts and federating means of the Member States. Such an EU NAVWAR capability will contribute to the unlimited and uninterrupted access to the Galileo PRS worldwide (Decision 1104/2011/EU), on EU Member States territory and abroad during operations or missions.

Scope

The proposals must aim at developing a comprehensive EU NAVWAR capability, relying on space-based and ground-based surveillance, and complementing current European efforts to strengthen the future Galileo PRS service resilience for military applications and the development of the user segment used by the forces of the EU Member States. To this end, the proposals must address the NAVWAR overall system, including a modular NAVWAR information-management system, networked with NAVWAR subsystems and NAVWAR PRS sensors. The objective is to achieve overall global capability dealing simultaneously with resilience, surveillance, and offensive measures. Different NAVWAR PRS sensors, along with common interfaces, must be determined and combined in various use cases as NAVWAR subsystems (integration environments) to create a NAVWAR network. They must include Galileo as PNT source and Galileo PRS as a PNT service. The interfaces with other communities and stakeholders must be specified as part of the proof of concept.

The proposals must address the following crucial development strands:

1. support, via a space-based and ground-based NAVWAR surveillance system, the nominal performances of GNSS/PRS receivers in a contested and hostile electromagnetic environment:
   - allowing localization, identification and characterization of main threats, and monitoring of GNSS signals;

[46] Public Regulated Service.

- including the federation of NAVWAR operational centres (used by the Member States based on a NAVWAR information-management system for data exploitation and C2 of the network of NAVWAR sensors/subsystems (space and ground)), that will support the implementation of the overall NAVWAR capability (including PRS);
- including interfaces with other communities in order to exchange NAVWAR situational awareness picture and recommended offensive measures;
- including common standards for NAVWAR surveillance interoperability among EU Member States;

2. develop a modular PRS mobile receiver concept[47] able to contribute to the network of NAVWAR sensors/subsystems, and possibly benefit from the overall capability; functional requirements related to data content and delivery aspects, must in particular properly identify typical performance features[48] that must be made available to the user segment through a secondary channel or in a server-based GNSS service approach:
   - this must include a risk reduction phase for maturation of miniaturized, modular, and SWaP-C optimized mobile PRS technologies and analysis regarding availability by EU vendors;
3. implement anti-jamming and anti-spoofing technologies in secure innovative architectures to support PNT superiority.

All aforementioned work strands must take into account on-going EU funded initiatives, in particular Galileo 2nd generation, and complement the on-going EDIDP GEODE developments/designs with modular miniaturized form factor PRS technologies, in particular for small platforms or mobile use cases.

The proposals must provide an efficient answer to the following operational concerns:

- regarding NAVWAR surveillance:
  - detect illegitimate activities (*e.g.* jamming, spoofing) in GNSS frequency bands distinguishing between intentional or unintentional sources;
  - provide RF and content analysis of detected signals;
  - geolocate and track sources of malicious activities;
  - deliver a NAVWAR situational awareness picture;
  - support EU GNSS and Galileo signal-in-space monitoring;
- regarding offensive measures:
  - provide analysis tools for the recommendation of offensive NAVWAR measures;
- regarding system architecture:
  - identify the added-value of a NAVWAR sensor network;

[47] Able to meet the integration in different hosts with a minimum SWaP-C (Size, Weight and Power - Cost) feature for a wide range of mobile user-segment applications in a military cross-domain framework.
[48] Performance requirements must be set for specific performance features in the trade-off engineering process.

- establish the role of Galileo PRS equipment in the overall NAVWAR capability;
- provide a perspective on offensive capabilities accessible via PRS equipment;
- provide, via the PNT sensors, information on the Quality of Service of PRS and OS[49] signals;
- provide options for the exchange of the NAVWAR situational awareness picture between NAVWAR centres and to electronic warfare (EW), Cyber or other communities.

Targeted activities

The proposals must cover the following activities as referred in Article 10(3) of the EDF Regulation:

- studies, such as feasibility studies to explore the feasibility of new or improved technologies, products, processes, services and solutions;
- the design of a defence product, tangible or intangible component or technology as well as the definition of the technical specifications on which such design has been developed which may include partial tests for risk reduction in an industrial or representative environment;
- the development of a model of a defence product, tangible or intangible component or technology, which can demonstrate the element's performance in an operational environment (system prototype);
- the testing of product, tangible or intangible component or technology.

In particular the proposals must address the following tasks:

- general considerations:
  - definition and description of the general EU NAVWAR concept and gathering of user requirements;
  - functional and performance analysis of typical scenarios (to be defined) to allow the detection and localization of jammers and spoofers, based on both system-scale and sensing payloads simulations;
  - identification of various EU NAVWAR system architectures depending on KPIs[50] coming from user requirements (*e.g.* RF sensitivity, localization accuracy, refresh rate of information…);
  - studies regarding standardization and interoperability recommendations;
- NAVWAR sensors:
  - design, prototyping and evaluation of various types of sensing payloads (including PRS);

[49] Operating Systems.
[50] Key Performance Indicators.

- study and design of a PRS mobile receiver, including study, prototyping and testing of identified technological hard points able to support, and possibly benefit from, the overall NAVWAR capability as part of the network of NAVWAR sensors/subsystems for dedicated military applications and use cases (dismounted, hand held, wearable or miniaturized integration, *etc*.);
- study and implementation (proof of concept) of NAVWAR capabilities into PRS receivers;

- NAVWAR subsystems:
  - in-orbit demonstration of (a portion of) the space-based NAVWAR surveillance capability;
  - study and implementation (proof of concept) of a common interface for various types of PNT/PRS-based NAVWAR subsystems in order to support the communication with the NAVWAR information-management system;
  - study, design and development (proof of concept) of integration environments for a network-based recognised picture of the NAVWAR situation for mobile applications (smart architectures, mobile radios) including housing, antennas, electronics and GUI;
- NAVWAR overall system
  - study, design and development (proof of concept) of the federation of NAVWAR operational centres, including algorithms prototyping and implementation of the NAVWAR information management system, to demonstrate NAVWAR situational awareness (elaboration and update of a NAVWAR recognised picture);
  - study and implementation of a PoC for a common interface and analysis tool for the NAVWAR information-management system to:
    - manage the network of NAVWAR sensors/subsystems;
    - recommend NAVWAR offensives measures (including at PNT sources level);
    - interface with electronic warfare (EW), Cyber, Competent PRS Authority (CPA) and other communities (NAVWAR measures and exchange).
  - comprehensive demonstration of a situational awareness picture that rely on a NAVWAR sensors/subsystems grid network composed of mobile, ground and space equipment including Galileo PRS receivers.

Functional requirements

NAVWAR sensors:

- the modular miniaturized and SWaP-C optimized PRS receiver concept, including study, prototyping and testing of identified technological hard points, should support the integration in different hosts (NAVWAR subsystems). Solutions should support standard

interface (including ICD[51]) or implement an Open Systems Modular Architecture for integration in different environments;

- the security architecture (proof of concept) should support smart architecture or server-based solutions for a wide range of mobile applications (encompassing high mobility domains).

NAVWAR subsystems:

- the sensing payload should cover all current GNSS frequency bands (Galileo, GPS, Glonass, Beidou…);
- the satellite system should allow to cover every region, worldwide, at least once every 2 days;
- the ground control segment of the satellites should implement an interface with the NAVWAR information-management system that supports data distribution to the analysis tool;
- the GUI for each component in charge of displaying NAVWAR information should be user-friendly;
- peripheral technology developed for the mobile use cases should be able to support the contribution to a network of NAVWAR sensors/subsystems;
- in order to enable the NAVWAR sensors/subsystem network, all considered solutions mobile and satellites, should be able to identify jamming and spoofing events and then transmit (at least by defining an ICD) the data for further analysis by the NAVWAR information-management system;
- the mobile solutions should cover Galileo PRS on both frequencies and all GNSS open signals frequencies;
- the mobile PNT solution may also encompass integrated non-GNSS and/or non-RF technology using sensor fusion algorithms and artificial intelligence;
- a small passive antenna-technology addressing relevant operational environmental conditions may be developed;
- the solutions should encompass a software defined approach and show compliance and interoperability with standardized PRS receivers already developed, able to be upgraded during their operative life through continuously updated libraries.

NAVWAR overall system:

- the system should geolocate and track, with an average accuracy better than 5 km, RF signals emitting at least 10 W power in GNSS frequency bands;
- the system should include all tools (*e.g.* graphical, algorithms…) in order to understand the NAVWAR picture on any area of interest. Especially, the system should handle

[51] Interface Control Document.

chronological events to apprehend the evolution of the NAVWAR picture (including standardization of a recognised picture of the NAVWAR situation);

- an analysis tool should be developed to allow performance analysis of Galileo PRS and other GNSS signals to detect jamming and spoofing based on the data provided by the network of NAVWAR sensors/subsystems;
- the NAVWAR information-management system should implement a modular concept that includes common interfaces for the exchange of:
  - information with the network of NAVWAR sensors/subsystems;
  - recommendations and tasking for NAVWAR offensives measures (including PNT sources);
  - recommendations for NAVWAR resilience categories towards the mission planner;
  - information with EW, cyber and other communities;
  - information with CPAs internal systems;
- a common ICD (*e.g.* messages) for the system should be defined to address the whole network of NAVWAR sensors/subsystems and the NAVWAR overall capability (resilience, surveillance and offensive measures);
- the system should include a function to store raw data and refined data;
- the system should be able to provide a standardized NAVWAR analysis to the user who requests it, through a predefined and automated process that will make available *added-value information* to the PRS user segment via space and/or terrestrial communication links. *Added-value information* could be for example (not exhaustive list):
  - availability of required accuracy (probability that PVT[52] data is provided with a certain level of accuracy);
  - EMI[53] localization accuracy (error of location measurement of an interfering signal);
  - GNSS-denied accuracy (error in PVT data when there is a loss of GNSS signal reception).

  Innovative solutions should consequently be envisaged (study, design, proof of concept) to exploit "smart" or "server-based" PRS service architecture [54] able to make the aforementioned added-value information available to the end user;
- the system should implement specific training functions in order to allow exercises without impacting the operation of the system.

Organisation:

- a risk-assessment taking into account all end-to-end data flows addressing relevant operational environments and identifying residual risks should be established;

[52] Position, Velocity and Time.
[53] Electro Magnetic Interference.
[54] Respectively with specific PRS crypto technology - or without any - built into the receiver to implement security functions.

- a concept to address the full NAVWAR capability (resilience, surveillance and offensive measures) should be established with the support of the Ministries of Defence of the participating Member States.

Expected impact

- Strengthen EU military resilience regarding NAVWAR offensive actions.
- Contribute to the autonomy of the European defence industry and to the security and defence interests of the Union.
- Provide essential technologies for EU defence interoperability.
- Contribute to Galileo services (especially PRS) monitoring and assist relevant spectrum monitoring agencies.

2.7.2. Topic EDF-2021-SPACE-D-EPW: European protected waveform and accompanying technologies for resilient satellite communications against jamming

Space is one of the global commons and an emerging operational domain at the same time. It provides unique options to deploy capabilities, which deliver services increasingly indispensable for military purposes and operations. This situation is going to produce specific new threats and challenges. The access to space has to be duly monitored and eventually protected as well as the capabilities already deployed and operating in orbit.

In today's military applications supported by satellite communications, security, resilience, information assurance and link efficiency technologies are inextricably linked. Military operations are becoming more complex as conflict areas grow more dispersed on a global scale, with a growing need to support a diversity of on-the-move, on-the-pause and fixed platforms. At the same time, security threats are becoming more apparent, raising concerns that nations, terrorist groups, criminals and individual hackers can jam, interrupt and endanger military operations. The challenge is to meet, in a secure and guaranteed way, the increased demand for raw capacity generated by continuous growth in space data rate requirements for military purposes. This covers the trend of higher mobility as well as the filling of current coverage gaps (*e.g.* over the Polar Regions).

Specific challenge

The complexity of diverse and dispersed military operations translates into requirements to have access to complex global satellite communication networks with a mix of different satellite constellations, networks and services to support a wide variety of military applications. Security and resilience, as key features in today's military use of space, have to be paired with efficient technologies in order to cope with the increased data demand through high-bandwidth consuming services that need to be supported by satellite communication, such as ISR and situational awareness, the growing use of drone applications, and the need for seamless and real-time end-user connectivity during operations. However, these wide-ranging and complex requirements face an increased risk of ill-intentioned acts including cyber-

attacks against military satellite communication networks such as jamming, signal detection and spoofing and interception attempts.

The key element to tackle these security challenges is the implementation of an integrated multi-layered security and resiliency approach for next-generation defence satellite networks with a fully European protected waveform and accompanying technologies for satellite communications resilient against ill-intentioned acts. This European Protected Waveform (EPW) must respond to the operational requirements and the identified security challenges, and considerably enhance interoperability during joint operations with allies whilst assuring seamless operations and protection of the satellite link.

The great majority of Member States do not have autonomous access to secure satellite communication waveforms, although they also engage in military operations in a national or multinational context (EU, NATO, UN peacekeeping, *etc.*). The investment for developing a protected waveform cannot be carried out by a single nation alone and requires a multinational development approach in a European context with the aim to establish an interoperable European Protected Waveform.

The European Protected Waveform is fully in line with and would contribute to the EU ambition to set up resilient satellite communication services for governmental and institutional security users and to achieve increased EU autonomy in space, as outlined in various documents from the Space Strategy for Europe, to the EU Global Strategy and the current EU Space Programme for 2021 to 2027. In the EU Capability Development Plan (CDP) of 2018 space has been identified as one of eleven EU capability development priorities. Following the CDP, in the Strategic Context Case for Space Based Information and Communication Services, established with and approved by the EDA participating Member States, a European Protected Waveform has been identified as a gap and the development of an EPW has been agreed as a short-time activity to fill this gap. More recently, in the Commission Action Plan on synergies between civil, defence and space industries satellite based secure communications and connectivity was again identified as a key activity and future flagship action with focus on standardisation and innovation, aiming at providing a ‘resilient connectivity system allowing Europe to remain connected whatever happens, including large-scale cyber-attacks’.

Scope

The proposals should address the development of an EPW for satellite communications as well as the complementary ancillary technologies addressing security and resilience that can be used by different EU Member States individually or together in a joint operational context (EU, NATO, multi-nation missions).

The EPW must be able to operate in the complex military operational environment described in the specific challenge and bring a solution to the corresponding challenges. The proposals must not be limited to the work towards the development of a waveform but must also include complementary ancillary technologies to provide an integrated multi-layered security and resilient approach to military satellite communications.

The proposals must keep the following five (5) key considerations in mind:

1/ Innovation

The EPW development must not just be a copy and paste of existing waveform solutions, licenses and technologies. The proposed EPW must be ambitious and innovative, combining the individual strengths of different Member States or associated countries and of different members of the European satellite communication industry. The EPW program must be open to support future requirements and capability needs.

2/ European autonomy and cooperation between Member States

The EPW must be capable of increasing the autonomy of the Union and of reducing the dependence on non-European satellite communication technology for military operations with mission critical and sensitive information. At the same time, it must allow for interoperability between Member States in a joint operational context in order to exchange mission critical information and improve the efficiency of the operations.

3/ Affordable and efficient satellite services

The EPW must be affordable and include the most efficient satellite communication waveform, networking and equipment technologies to reduce OPEX (*e.g.* bandwidth, planning resources) and CAPEX (equipment cost) compared to current existing expensive (proprietary) military satellite solutions. The EPW must include already available innovative Commercial Off-The-Shelf (COTS) satellite communication technologies (*e.g.* DVB-S2X waveform standard) in combination with the latest security and resilience technologies. There must no longer be a trade-off between the efficiency of the waveform and security. As such, high throughput demands must be achieved even with small satellite terminals using a limited amount of satellite bandwidth (in contested and/or congested environments).

4/ Flexibility and scalability

The EPW must be portable on different software defined modems with different form factors (board, modem, terminal), different platforms (fixed, on-the-move, on-the-pause) and be used across multiple types of satellite communication networks, different types of multi-orbit satellite constellations (LEO, MEO, GEO, HEO, high- and very-high throughput satellites, spot beams, regional and global beams) and different network architectures (VSAT, point-to-point, mesh) also considering possible extension to future EPW processed satellite transponder employment. At the same time, the EPW must be operational in different satellite frequency bands (at least C-band, X-band, Ku-band and (mil- and civ-) Ka-band) with extension to Q-/V-band to support future military constellations of communication satellites and exchange, broadcast, multicast, unicast or relay a large range of satellite services and applications from low to very high data rates. Interrelations with the ESSOR (European Secure Software defined Radio) project must be investigated in order to avoid unnecessary duplications and maximise synergies between these projects.

5/ Multi-layered security and resilience

The EPW must be embedded in an integrated multi-layered secure and resilient approach to increase the protection of mission critical military satellite networks. Based on different threat

analysis and Concept of Operations (CONOPS) scenarios, the EPW development must focus on building satellite networks that are resistant to the increasing security threats in terms of jamming, interference, interception and cyber. In addition, satellite link outages caused by rain fade, atmospheric conditions or on-the-move communication challenges must be reduced to a minimum. The EPW activity must investigate how different security levels can be offered towards different military end users depending on their security requirements and their daily operations (as well as the budgets available).

The scope must be extended to anti-jam, multi-band/multi-frequency terminals, network diversity and network security technologies to ensure end-to-end secure and resilient military satellite networks, fostering the possibility to exploit dedicated EPW processed transponders (*e.g.* on board frequency de-hopping, re-hopping capability) in order to even protect user access to satellite resources.

Targeted activities

The proposals must cover the following activities as referred in Article 10(3) of the EDF Regulation, not excluding possible downstream activities eligible for development actions if deemed useful to reach the objectives:

- studies, such as feasibility studies to explore the feasibility of new or improved technologies, products, processes, services and solutions;
- the design of a defence product, tangible or intangible component or technology as well as the definition of the technical specifications on which such design has been developed which may include partial tests for risk reduction in an industrial or representative environment.

In particular, the proposals must cover the following tasks:

- **study** phase:
  - feasibility study, use cases, and CONOPS definition;
  - threat and vulnerabilities assessment, risk analysis, and identification of counter measures and security requirements (*e.g.* anti-jamming, network diversity, multi-band/multi-frequency terminal and network security solutions);
  - system specification, Detailed Requirements Review (DRR) and architecture definition; benchmarking of existing solutions in the market;
- **design** phase**:**
  - detailed design of the system, including the Preliminary Design Review (PDR) and finishing with the Critical Design Review (CDR);
  - development of an EPW simulator to de-risk the development of subsequent technological demonstrators;

- the development of small-scale technological demonstrators to support decision making during the design phase. The demonstrators must:
  - demonstrate the functionality of the waveform used in different operational use cases alongside the adjacent security and resiliency technologies (multi-frequency terminals, *etc*.) allowing testing against multiple instances of interference, jamming and interception, *etc*. but also in context of different satellite types, different architectures, and platforms (on-the-move, on-the-pause and fixed). The use of drone technology to test the terminal and waveform technology is encouraged;
  - reproduce the operational environments in terms of usage and threats;
  - be set-up initially a lab environment, but should then be followed by a real satellite test with outdoor satellite terminals simulating operational use cases. Military end-users should be invited to witness the demonstrations and to provide feedback.

The end state must be an EPW standard for satellite communication, a so-called Blue Book, comparable to other communication waveform standards that can be implemented by industry on their baseband solutions (terminals, modems) and integrated in the Member States military networks. It must take into account the accompanying anti-jamming, network diversity, multi-band/multi-frequency terminal and network security solutions, based on traditional and new generation satellite systems that could implement the EPW communication standard in SW defined radio solution on board.

Functional requirements

In accordance with this integrated multi-layered security and resiliency approach for military satellite networks the EPW development should fulfil requirements at the level of the waveform, the satellite baseband equipment (terminals, modems, hubs, networks) and end-to-end satellite network level including multi-band/multi-frequency terminals, anti-jamming technologies, interference mitigation, network diversity, network security and cyber technologies. The demarcation point is the edge router of the satellite network which connects the hubs, gateways and modems with outside networks or the internet. With this approach it will be feasible to implement the EPW also on existing and operational telecommunication satellites.

Protected waveform requirements

The EPW should:

- be defined as a standard to enable interoperability in joint operations. Multiple terminal vendors should be able to support the EPW and be compatible;
- be affordable, based on the best practices of COTS and government or military-grade waveforms;
- implement the most efficient SATCOM technologies to obtain the best performance out of a satellite link;
- support a range of different multi-orbit satellite constellations ((V)HTS, wideband, military, commercial, government, GEO, MEO, LEO), satellite architectures (pure

transponder, partially or fully processed) and frequency bands (C-band, X-band, Ku-band, (mil- and civ-) Ka-band) with extension to Q-/V-band to support future milsatcom constellations) and have the capability to roam across the different satellite networks in a seamless manner;

- be easy to port on other Software defined modems or hubs;
- flexible to support multiple governmental and defence applications that require different levels of security;
- consider a growing amount of on-the-move and on-the-pause platforms connected over the satellite with a need for mobility features (Doppler compensations, spreading modulation, small and flat antenna support, beam switching, beam hopping, *etc*.);
- operate in GNSS-denied environments;
- provide adequate protection against intrusion, hacking, jamming, traffic monitoring and eavesdropping (Low Probability of Detection – LPD / Low Probability of Interception – LPI);
- masking and obscuring traffic anti-jamming patterns across the satellite link that could give away activity related information on ongoing operations and assets;
- consider a wide range of throughput requirements and satellite bandwidth sizes (symbol rates);
- offer seamless and resilient satellite links against fading effects, interference (intentional and unintentional), shadowing effects and jamming (fixed and sweeping);
- be capable of supporting different service models such as pooling and sharing.

Multi-layered security and resilience requirements (extended capabilities)

- the EPW is embedded in an integrated multi-layered security and resilience approach which increases the protection of mission critical military satellite networks. As such an overall approach needs to be envisaged to align the EPW development with the complementary security and resiliency technologies for ground and space segments;
- anti-jamming technologies that allow to detect, mitigate, prevent and predict jamming efforts by third-party adversaries. This can be tackled through spectrum monitoring, geolocation and network management technologies working together with nulling or interference excision technologies as well as Anti-Jam waveform capabilities as Direct Sequence Spread Spectrum, Frequency Hopping Spread Spectrum and beam forming technologies;
- network diversity, redundancy and geo-redundancy technologies to increase the resilience of the military satellite network as well as multi-access capabilities (hybrid LTE/5G/*etc*.) with intelligent routing;
- multi-frequency terminals and antenna systems that can dynamically steer its radiation pattern accordingly to connect to another satellite in a different frequency and satellite orbit to increase network resiliency. Both fixed, on-the-move and on-the-pause terminals,

manpack and antenna systems need to be considered as well as different types of antenna technologies (*e.g.* parabolic, electronically steered, phased array, flat antennas, *etc*.). The secure connection and interface between antenna system and baseband needs to be taken into account as well;

- network and ground segment technologies that improve the cyber hardening of all satellite platform elements including protection against possible hacking, network intrusion, *etc*.;
- protection technologies against hostile action (*e.g.* jammers, intrusion and eavesdropping transmission) for critical satellite datalinks, improving signals protection and integrity;
- providing future proof interfaces and complementarity to upcoming disruptive security technologies such as quantum, self-healing networks, *etc*.;
- be open towards upcoming and existing EU-based pooling and sharing programs (*e.g.* GovSatCom) and satellite constellations (EU Secure Space Connectivity System initiative that is under study) and ready to be integrated in these concepts.

Baseband equipment requirements (hubs, modems)

- the right implementation of the terminal will determine the success of the EPW. The flexibility and the affordability of the terminal are key considerations. Hence, a Software Defined Mode type of baseband equipment should be pursued;
- the baseband infrastructure (hubs and modems) needs to cover multiple architecture types of networks (point-to-point, point-to-multipoint, mesh) and satellite (wideband, spot beam, mix of both, transparent, processed) architectures;
- the EPW should operate on Software Defined hardware from different vendors that will be selected by nations, government and defence agencies or institutions, depending on their preference or acquisition processes;
- the EPW should include the ability to receive and transmit various modulation methods using a common set of hardware;
- the EPW should be future-proof, easy to upgrade and change configurations (over-the-air) with the ability to alter functionality by downloading and running new software at will, in order to repurpose the modem for a new application;
- the EPW should be affordable and include the latest efficiency satellite waveform, networking and equipment technologies to save OPEX (reduce bandwidth costs, save resources for planning) and CAPEX (save on equipment cost) compared to existing expensive military satellite modems;
- the EPW should consider Size, Weight and Power (SWaP) constraints for on-the-pause and on-the-move platforms and unmanned systems. Modems and terminals should be easy to transport and deployed and use a minimum amount of power;
- the EPW should be deployable in different environment conditions and on different platforms (land, sea or air);

- the EPW should be available in different form factors (OEM cards, rack units or rugged terminals);
- the EPW should be transparent for national encryption standards and externally encrypted data, and capable of integrating on-board modules for encryption technology;
- the EPW should be resilient and maximize service availability to ensure continuity of seamless operations;
- the EPW should have performances considering the throughput demands of today and the future;
- the EPW should support pooling and sharing service models of both waveform and equipment that can be implemented for different operations;
- the EPW should take into account the new use cases and technologies linked to 5G, Machine-to-Machine (M2M), Internet-of-Things (IoT), orchestration, cloud-services, the connected soldier and smart defence.

Expected impact

- Availability of a critical enabler for EU Member States defence forces and CSDP operations and missions in providing scalable secure and resilient communications with protection against intrusion, hacking, jamming, traffic monitoring and eavesdropping.
- Full interoperability between different demanders and suppliers of satellite communication in support of military operations and missions.
- Secure, guaranteed and affordable access to satellite communications for all Member States and CSDP missions and operation.
- Strongly increased European autonomy in satellite communication for defence users and no longer dependency on support from outside the EU for the transmission and exchange of mission critical and sensitive information.
- State-of-the-art technological solution in line with the latest satellite innovations and initiatives such as 5G, broadband connectivity, small LEO/MEO satellites, connected vehicles and Internet of Things.
- Scalable towards existing and planned EU-based pooling and sharing programs (*e.g.* GovSatCom) and satellite constellations (EU Secure Space Connectivity System initiative that is under study) and ready to be integrated in these concepts.

2.8. Call EDF-2021-DIGIT-R: Artificial intelligence

Proposals are invited against the following topic:

- **EDF-2021-DIGIT-R-FL:** Frugal learning for rapid adaptation of AI systems.

Budget

The Union is considering a contribution of up to EUR 18 500 000 to support proposals addressing the abovementioned topic and its associated specific challenge, scope, targeted activities and functional requirements.

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

2.8.1. Topic EDF-2021-DIGIT-R-FL: Frugal learning for rapid adaptation of AI systems

Specific challenge

In times of real-time information availability and exchange, and increasing complexity of situations, artificial intelligence (AI) has become an essential driver for new competitive system solutions. Future military capabilities will include a significant share of systems that will make massive use of AI techniques.

Modern AI systems based on Machine Learning and especially Deep Learning techniques usually require many labelled data points to reach acceptable performance. Furthermore, they can suffer from inconsistent behaviours, such as high-confidence failures, or failures in trivial cases. More generally, improving AI systems to take into account new data requires extensive testing by expert developers to avoid regression. These issues severely impact their availability for defence systems, which are characterised by the lack of data, for instance when dealing with enemy intelligence, and by the need for trustable results and rapid adaptation, including from data that cannot be shared with system developers for confidentiality reasons or because of poor connectivity. This is especially important when the information to manage is highly variable or unpredictable and high adaptability is needed.

The challenge is to develop new Artificial Intelligence methods that are able to make use of less training data than current state-of-the-art deep learning algorithms while maintaining similar performance, to provide better control over the output space in order to ensure a more consistent behaviour, and to limit the development efforts when adapting systems to new data. These methods must prove their worth on realistic and challenging use cases representative of military operations.

Scope

The aim is to tackle the problem of robustness and frugality in military AI software components to facilitate the development of new systems and their adaptation to the evolution of their environment, including from user supervision, for a reasonable cost, with minimal intervention from expert developers, and without regression. State-of-the-art research on transfer learning, zero- or few-shot learning, active learning, domain adaptation, hybrid AI and other relevant topics should be leveraged to propose new methods to improve AI-based methods, while preserving high performance.

Targeted activities

The proposals must cover the following activities as referred in Article 10(3) of the EDF Regulation, not excluding possible downstream activities eligible for research actions if deemed useful to reach the objectives:

- activities that aim to create, underpin and improve knowledge, products and technologies, including disruptive technologies for defence, which can achieve significant effects in the area of defence.

The proposals must address in particular the following objectives:

- design of relevant military use cases where trustworthy and frugal AI algorithms are needed (*i.e.* targeting specific tasks for which data-greedy algorithms are currently outperforming other methods), and for which representative data can be collected and performance can be measured in an objective way;
- development of new methods for reducing the need for data and supervision to train and adapt AI systems (and simultaneous monitoring of the state of the art, which is important in this quickly evolving domain but should take place as a background activity integrated with system development), for example through:
  - simulation and generative models;
  - transfer, semi-supervised, self-supervised, and active learning;
  - hybridisation with user-defined rules;
- development of new methods for improving robustness guarantees by design, for example through:
  - new algorithms increasing the robustness of existing neural networks methods that are intrinsically not robust;
  - evaluation and surveillance of both the output space and the environment;
- implementation of benchmarking experiments on the use cases to demonstrate the advantages and drawbacks of the proposed methods.

Functional requirements

The proposed solutions should fulfil the following requirements:

1) General
   - for each use case addressed, several approaches should be explored by different research teams;
   - the proposed techniques should be presented in the proposals;
   - all systems addressing a given use case should be benchmarked using the same experimental protocol (metric, data, train/test split, *etc*.) in order to ensure comparability;

- in all experiments, several runs should be performed in order to provide the means and variances of system performance estimates;
- a strong and solid open source strategy has to be defined to ensure sharing of the generic results, functions, software with a license compatible the further development and commercial exploitation of the results (*e.g.* ePL, L-GPL, *etc*.);
- for at least one use case, means to reproduce the experiments in a comparable way should be ensured beyond the project, by publishing as open data the use case description, associated dataset and metrics. The consortium member(s) guaranteeing this sustainable availability should be clearly identified;
- possibilities and conditions to provide further use-case data and means to reproduce experiments and benchmarks with internal methods, in particular for national authorities and their technical centres, should be described. The consortium member(s) ensuring this should be clearly identified.

2) Use cases

- use cases should be defined and precisely described, including a description of the data to be collected and used for the experiments and a description of the metrics to assess progress;
- use cases should revolve around one or several of the following topics:
  - situation awareness and intelligence (ATD/ATR, monitoring, change detection, data fusion…), for multiple vectors (robot, UxV, vehicle) and sources (multimodal and/or multilingual);
  - operational C2 (decision aid, threat assessment, effect prediction, movement coordination, mission planning…);
  - mission equipment (autonomous vehicle, delocalised decision…);
- use cases should be representative of modern military conditions, by using sufficient amounts of real or realistic data;
- use cases should be challenging, *i.e.* existing methods from academic and/or industry state-of-the-art should not be close to a saturation point (*e.g.* a 100% success rate for a simple image recognition use case, without challenges, on a basic set of simulated data, is not relevant);
- the process by which an end user could adapt a system to fit its own data or rules should be investigated, in order to determine whether it is possible to do so without expertise in AI;
- systems should be resilient to inconsistent inputs and to attacks (adversarial attacks, data poisoning…).

3) Frugal AI

- frugal AI systems should require smaller amounts of data than traditional state-of-the-art ones to offer similar performances;

- systems should be benchmarked with respect to the cost of data creation (in particular as a function of the number of labelled and unlabelled examples) and/or system supervision (*e.g.* minimal amount of supervision needed to provide a correct output).

4) Robust AI

- robust AI systems should be able to ensure some predefined properties and behaviours. When adapting to new environments, they should ensure non-regression and possibly guide user supervision;
- systems should be benchmarked with respect to these abilities and offer enhanced performance compared to traditional stat-of-the-art systems (by avoiding failure in trivial cases or inconsistent behaviours while maintaining performance in other cases).

Expected impact

The expected impacts are to:

- accelerate the introduction of robust AI in military systems;
- increase trust of experts and end users in AI systems;
- increase system performance and resilience;
- enhance technological autonomy.

2.9. Call EDF-2021-DIGIT-D: Cloud technologies

Military operations require higher flexibility and mobility to gain and maintain the initiative. The capability to securely, timely and robustly communicate over all battlespace domains is key for information superiority, mission management and decision support. Therefore, the development of a common shared Information Space with a "Cloud of Clouds" approach, leading to a Multi-Domain Operations Cloud (MDOC), is needed. The ambition is to combine existing and future systems into a federated network and collaborative services in order to enable and support Command and Control for multi-domain warfare. Furthermore, the data collected across domains will open up future opportunities to develop artificial intelligence (AI) enabled solutions for defence.

Proposals are invited against the following topic:

- **EDF-2021-DIGIT-D-MDOC:** Military multi-domain operations cloud.

Budget

The Union is considering a contribution of up to EUR 40 000 000 to support proposals addressing the abovementioned topic and its associated specific challenge, scope, targeted activities and functional requirements.

Up to one action may be funded under this call.

2.9.1. Topic EDF-2021-DIGIT-D-MDOC: Military multi-domain operations cloud

Specific challenge

Information transcends operational domains and multiplies the size of effects in combat. Warfare is no longer segregated into specific domains, as information sharing lies at the heart of cooperation and boundaries of the individual domains are blurring.

A collaborative, efficient and secure information management across land, sea, air, space and cyber domains is key for operational superiority, mission management, decision support, and for future capability development in the area of AI.

An overall military advantage and information superiority will be achieved through complete situational awareness based upon current data from all available sources. In modern warfare, the right information at the right place and at the right time can make the difference in a contested military environment as well as information gaps in the non-real-time reporting chain. Furthermore, if data is collected, stored and made securely available for the purposes of later developing AI solutions, its value would be further maximized.

Currently, information is not adequately shared in military systems and is rather kept enclosed in systems or sub-systems interconnected by local and domain specific interfaces. The lack of information sharing and coordination across all military domains is amplified by the existence of different data models limiting appropriate information exchange and exploitation. This situation may lead to different information interpretation, thus producing multiple situation pictures of the same situation and ultimately allowing taking uncoordinated decisions.

Additionally, the digitization in every domain progressively introduces high-performance systems creating increasing amounts of data that needs to be distributed and shared among various combat actors from tactical to strategic levels. This evolution overwhelms the architecture and networking capabilities of current generation systems and creates a challenge for a new generation operations cloud. Furthermore, the lack of specific rules governing data collection and curation hinders the possible re-use of these data for the training of AI solutions.

The civilian cloud versions use very-high-speed networks for information access and synchronisation and take advantage of decentralized resources in multiple data centres. In the military environment, specific constraints exist (such as high mobility with no reliance on support infrastructures, transmission security and electromagnetic contested environment, limits in networks data rate and availability, limits in local computer and storage resources, disconnected modes, environment and hardening constraints, *etc.*) that impose a challenge on the direct usage of the civilian solution. In addition, even if many classical IT services (messaging, chat…) are close to their civilian counterparts, operational users request specific applications and services which need to be shared for a real federated multi-domain cooperation (*e.g.* C2 services, ISR services, tactical situation or logistics, training and exercises).

As commercial cloud concepts and the underlying networking models cannot be applied (or can only partially be used), a specific architecture with cloud technologies has to be set up for military purposes reflecting the needs for special adaptations, especially for the operational

and tactical use cases. However, cyber ranges across multiple EU Member States have the relevant infrastructure that would allow them to act as secure data repositories and for training and testing (*i.e.* sandboxing) AI solutions.

Scope

Proposals should address the development of a multi-domain cloud architecture for defence and an associated technological demonstrator, providing a common shared information space and federated services enabling multi-domain operations.

The ambition is to combine data of existing and future systems through a federated network, shared cloud interfaces and implementation of the associated shared services. The ambition is also to make the data securely available for re-use in the promising field of AI.

MDOC must enable and support flexible combined and joint military missions and provide the capability for an accelerated and improved battle rhythm for military operations in a collaborative multi-domain warfare, ensuring adequate level of data protection.

MDOC must include three major components:

1) European virtual or digital platform;

2) Catalogue of end-user products and services;

3) Tools, interfaces and APIs.

The proposals must cover several key aspects and show how they will handle them:

- the specificity of requirements (operational/technical/environment/*etc*.) at strategic, operational and tactical levels and their impact on the architecture and solutions;
- the provision of secure and resilient services, multiple levels of security, hardware and software certification, cyber protection, data integrity solutions, *etc*.;
- the complementarity and synergies, avoiding duplication but bridging existing/upcoming single-domain cloud-based solutions, creating synergies between other already or soon-to-be launched cloud-based important initiatives and enhancing these efforts by enabling an advanced use of services and information across domains;
- the digital continuity aspect, *i.e.* a virtual environment enabling collaborative operations services across all domains and levels (strategical, operational and tactical);
- the need for an open architecture, designed in a modular way in order to accommodate specific requirements from tactical level to the different headquarter levels;
- the need to analyse and compare possible approaches to share data and services within military organisations, depending on the operation levels;
- the promotion of European standards regarding interoperability and information sharing, and the compatibility with other existing interface military standards such as NATO Federated Mission Networking (FMN);
- the synergies with European civilian cloud technologies where applicable;
- the synergies with the existing cyber ranges in the EU Member States.

Targeted activities

The proposals must cover the following activities as referred in Article 10(3) of the EDF Regulation, not excluding possible upstream and downstream activities eligible for development actions if deemed useful to reach the objectives:

- studies, such as feasibility studies to explore the feasibility of new or improved technologies, products, processes, services and solutions;
- the design of a defence product, tangible or intangible component or technology as well as the definition of the technical specifications on which such design has been developed which may include partial tests for risk reduction in an industrial or representative environment;

The proposals must address in particular the following tasks:

Studies

- detailed Requirements Review (DRR), analysing the main operational requirements from Member States at strategic, operative and tactical levels in terms of multi-domain operations;
- definition of the Concept of Employment (CONEMP);
- definition of use cases, defining actors, ways of operation, time constraints, expected data to be shared, existing or predicted services to be considered
- high-level feasibility study, identifying the main architecture options and their constraints (centralised /decentralised, cloud federation principles, multi-level security, multi-tenants, national sovereignty, including the possibilities of further utilising the existing Cyber Ranges in the EU for AI sandboxing…);
- definition of Governance;
- definition of a delivery model for the building blocks (who delivers what to whom and who supports);
- IT Platform preparation – small-scale version of the virtual platform to develop and to experiment the federated services (limited to a selection of services);
- IT and Core Services Modules development and integration in the virtual or digital platform;
- development and integration of the demo version of the catalogue; use of a limited set of services in areas to be defined (*e.g.* C2 or ISR – for illustration purposes only);
- technological demonstration of the federating platform and its key services.

Design

- conceptual design;
- architecture definition, laying down the overall multi-domain federated cloud architecture, including by partially using the existing infrastructure;
- system of systems specification, outlining platform related services;

- functional description, providing first version of the catalogue and the associated interfaces and APIs;
- standards and interoperability assessment;
- preliminary design tool to elaborate and customize architecture for each Member State.

Functional requirements

The proposals must include detailed descriptions and intended performances of solutions to the following requirements:

- describe the specific needs and requirements of different domains and levels of command, esp. in terms of information, interfaces and interoperability;
- apply and merge multiple domains from the battlefield to achieve a highly integrated network for communication, data capitalisation and resources sharing services;
- combine real-time data and non-real-time data networks and synchronize information for collaboration between land, sea, air, space and cyber platforms;
- enable the usage of big data analysis and its impact on cloud resources (computing power, storage) in the architecture options;
- enable the development of custom AI solutions on the available data and provide concepts to analyse the information with the given set of computing power from the tactical edge to the strategic level;
- allow for using the existing cyber ranges as secure data repositories and for sandboxing with the AI solutions;
- define the requirements for communication networks for data and control exchange;
- define rules for data collection, curation and secure sharing with the ultimate aim of achieving AI-ready data sets;
- adapt the quality of service and Information synchronization within the Multi-Domain Operations Cloud to the available network bandwidth and robustness over all levels of command, including the narrowband, disrupted/interrupted communication and as well as future networks on the tactical edge/far-edge level;
- provide a modular and scalable concept that accommodates the integration of ongoing multi/national programs and offers appropriate flexibility for a large European cooperation;
- define and specify network and information infrastructures, IT environment, cyber resilience, interfaces and initial services for the cloud of clouds and its three layers: strategic, operational and tactical;
- provide autarkic operations of single entities that ensure the continuity of operations in case of communication disconnections or interruptions;
- allow to shift operations between different nodes in the cloud of clouds to make full usage of the available resources;
- enable the prioritization of the tasks according to military hierarchical levels;

- allow a decentralised approach with distributed computing power of different quality;
- demonstrate the resiliency and the performance of the single services;
- guarantee protection of classified data and national sovereignty;
- ensure the continuity of solutions and services between core and far/edge levels;
- provide easy management of cloud infrastructure and services that integrate security rules;
- enable a European virtual or digital platform:
  - the platform should act as PaaS (Platform as a Service) and IaaS (Infrastructure as a Service) and should provide related services (PaaS, IaaS, Security and shared Core services);
  - the platform should be modular to allow various part or full implementations depending on national contexts;
  - the platform should support existing military tactical/operative level networks, tactical links and strategic networks;
- provide a catalogue of end-user products and services:
  - the catalogue should provide community-of-interest (COI) services and general COI enabling services, both dedicated to support connected customer applications for synchronization, consumption and data usage, *e.g.* (list for illustration purposes only):
    - AI and big data analytics services;
    - data confidentiality and integrity services;
    - consolidated situation data (real-time and non-real-time);
    - integration of the cyber domain monitoring and actions;
    - situational awareness data;
    - coalition shared data access;
    - workflows support services;
    - messaging services;
    - elaboration of operation plan templates and operation plans;
    - software-defined network services;
- develop tools, interfaces and APIs:
  - additional instruments should enable the development in the MDOC environment and ensure the open character of MDOC and its modularity;
  - identification of compliance with interoperability Standards (NATO STANAG and open standards);
  - APIs of the European Virtual or Digital Platform and of the catalogue of services;
  - interfaces with AI sandboxing data repositories.

Expected impact

The long-term expected impacts are to:

- provide Member States with enhanced, digitized and secure battlespace information across all operational domains (MDOC foundation);
- extend the collaboration capacities under development in each domain, through additional services and interfacing standards, which will allow joint operations with a minimal impact on single domain approaches;
- deliver standards, a cloud environment and a comprehensive portfolio of cloud services and products that will help Member States to build their national solutions;
- enable European armed forces to coordinate their activities over all combat domains based on the same situation data, regardless which application they use, and avoid mismatches of data in information exchange due to different data models used at the service layer, which would result in different situation pictures;
- improve operational processes to support cooperation between Member States;
- accelerate the battle rhythm of military operations based on real time exchange of data and synchronised collaboration between land, sea, air, space and cyber domains.

2.10. Call EDF-2021-ENERENV-D: Energy efficiency and energy management

This call aims at optimising the distribution and management of energy within or between defence systems, *e.g.* by making use of innovative solutions based on artificial intelligence.

Proposals are invited against any of the following topics:

- **EDF-2021-ENERENV-D-EEMC:** Energy independent and efficient systems for military camps;
- **EDF-2021-ENERENV-D-NGES:** Next generation electrical energy storage for military forward operation bases;
- **EDF-2021-ENERENV-D-PES:** Alternative propulsion and energy systems for next generation air combat systems.

Budget

The Union is considering a contribution of up to EUR 133 000 000 to support proposals addressing any of the abovementioned topics and their associated specific challenge, scope, targeted activities and functional requirements.

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

2.10.1. Topic EDF-2021-ENERENV-D-EEMC: Energy independent and efficient systems for military camps

Despite a constant improvement of their energy efficiency, a growing energy consumption of weapon systems and of their logistic footprint has been observed. This is mainly due to the

number of the vehicles, the huge requirements in mobility of force, the on-board electronic system, the soldier connected devices and equipment and more globally, the digitalisation of the battlefield. This increase in energy consumption should be achieved by means of new production such as renewable energies, hybrid powertrains or energy production, batteries and fuel cells. However, these new forms of consumption pose a challenge for their integration in weapon systems, for their technological development and for their logistics operational management. These multiple changes will lead to structural evolution regarding operational energy.

Nowadays, Forces mainly depend on fossil fuels to achieve their mission. This is even truer during operations. However, the question of the security of supply in future years faces two challenges:

- strategic issues linked to the access to resources;
- the climate emergency context, which requires the implementation of energy transition measures.

Part of the answer will come from the exploration and development of disruptive and new energy sources (synthetic fuels, hybridization, hydrogen, *etc*.), as well as the study of solutions allowing better management of resources and optimization of needs.

From an operational point of view, an autonomous military camp will integrate a wide energy source approach, with several different technological bricks (fuel cells, batteries, synthetic fuels small refinery, hybrid electric generator, deployable solar panel, *etc*.). From an industrial point of view, the collaboration between the partner Nations and the implementation of industrial standards would allow the creation of a European market for sustainable energy systems in defence applications and a better interoperability between allies engaged on the same theatre of operation.

The energy transition is an operational asset making it possible to be more efficient, aim at a better autonomy and strengthening the resilience of forces. It could also bring tactical benefits like the reduction of noise, thermal and electromagnetic signature.

Specific challenge

The specific challenges of the topic reside in:

- the need to reduce fossil fuel dependency in military deployable camps (support and mobility) without any drop of operational performances;
- the need to have a sustainable energy defence model with technical as well as operational standards agreed by European Nations (for overseas deployable field camp: energy requirement, different energies and tools needed or authorized to fulfil the mission);
- the need to optimize the involvement of Nations by considering all the studies, works and research carried out or ongoing within the framework of defence;
- the need to study the feasibility of different technologies to answer to the identified needs of the Member States ensuring the interoperability of systems and by taking into

consideration opportunities such as autonomy or resilience, but also the constraints such as cybersecurity;

- particularly the need to study projects involving hydrogen;
- the need to study all the issues of disruptive energies logistics: delivery, storage, distribution involving large quantities (particularly concerning hydrogen logistic);
- the adaptation for military requirements of already existing civilian equipment, as they will be used in specific climatic and operational conditions;
- the development of an operational simulation and planning system.

Scope

The proposal must address:

- benchmarking of the current industrial existing solutions and identifying the possible needs and constraints for adapting civilian products to the military operational conditions;
- benchmarking of the past and ongoing defence studies, research, and multinational military working groups' results, which represents a substantial work base;
- identification of the needs of the European Armies especially in an interoperable context for all types of energies including electrical network;
- study and implementation of technological solutions in order to allow the forces to reduce fossil fuel dependency in military deployable camps by integrating the logistics and financial aspect, and collateral benefits (for example, hydrogen fuel cells will produce water that could be used by human in extreme condition and in sensitive environments);
- study of the capacity to produce, transport, store, distribute and use hydrogen or hydrogen based synthetic fuels in military context and to power supply in fields operations;
- study on risk assessment (vulnerability, detections of such systems, how easy are to be replaced, possible collateral damage in case of destruction);
- study Artificial Intelligence (AI) for the camp's energy management system that hinder cyberattacks.

This action is a first step and the outputs could be used to set-up in a second stage a full-scale operational demonstrator of a deployable camp fulfilling interoperability between inter-allied armies and NATO, with a modular and easily deployable energy system and adaptable energy mix.

Targeted activities

The proposal must cover the following activities as referred in Article 10(3) of the EDF Regulation, not excluding possible upstream and downstream activities eligible for development actions if deemed useful to reach the objectives:

- studies, such as feasibility studies to explore the feasibility of new or improved technologies, products, processes, services and solutions.

The proposal must pay particular attention to the other R&D and dual-use on-going initiatives at Union level to avoid unnecessary duplication. The project should be as short as possible (typically two years) for allowing soon the building of the full-scaled operational demonstrator.

Studies:

- feasibility studies including an inventory and a state of the art of the finished or on-going projects and demonstrations of different technologies and emerging technologies in the military sector to reduce dependence on fossil fuels;
- architecture/topology study of the electrical power network taking into account the needs and the constraints of camps:
  - camp power grid optimal architecture from economic, environmental and technological point of view;
  - guarantee resilience, ensuring an adequate level of cyber protection, monitoring and incident management;
  - AI based optimal planning and control of camp power grid, AI based self-organizing power supply solution (*i.e.* microgrids) formed by mobile energy storages, distributed generators and electric vehicles;
  - modular approach aimed at managing and monitoring the microgrid, in terms of load balancing, blackout prevention and control, microgrid components fault detection and prediction, and sustainable maintenance strategy;
- study of a global energy military ecosystem including production, logistic and final uses (for example, in operational condition of a complete hydrogen chain, which includes production or transportation and filling centre, containers dedicated to hydrogen logistics and generator of electricity from hydrogen);
- study of the reliability and security of these systems (hydrogen/synthetic fuels, smart grid, microgrids, self-healing power systems, *etc*.) in order to validate the feasibility of deploying these types of solutions in operations areas (emergency energy use and auxiliary or primary power unit);

Work on standardization:

- establishment of European standards and specifications, which could be part of an EU standardization of deployable field camp.

An assessment of the procurement methodology:

- assessment of the procurement methodology to buy the systems by the MS taking in to account the economic scale effect.

A planning tool:

- studies for a tool to predict and simulate energy production / consumption for longer period of time and determinate the most efficient solutions (if possible implementing advanced

algorithms of machine learning, artificial intelligence, *etc*.) through the virtualisation of the energy consumption and production.

Training and Documentation:

- the use of new technologies in the context of military application, must also consider how the armed force will adapt to it. This will require a training and documentation well adapted to the specificity of the armed force.

Functional requirements

The proposed work should fulfil the following requirements:

- a study and a proposed energy architecture with lower fossil fuel dependency for a deployable camp, that means an operational military infrastructure (close to the threats), modular and the most autonomous possible in energy;
- an energy-system of a deployed camp should target the use of an energy mix, including a growing share of renewable energy while becoming also an operational military advantage:
  - by increasing the Energy autonomy of the camp:
    - with the use of renewable sources (wind, solar, geothermal, biomass, *etc*.);
    - if a power station is created, it should be able to be started and stopped by command;
    - by producing and storing its own electricity or sustainable fuel (*e.g.* Batteries, Hydrogen);
    - by ensuring energy efficiency and adaptability with a (DC or AC current) smart electricity grid and energy management system;
    - by implementing cogeneration of power and heat wherever is possible;
    - require a minimum of maintenance and simplify the supply chain of spare parts;
    - use cost-efficient solutions;
  - by increasing the operational capacity of the camp:
    - reducing the noise and detection/signature compared to the usual electricity generating units;
    - reducing the local pollution due to usual thermal engines by taking into consideration environmental and safety rules;
    - reducing the logistical convoys in fossil fuels;
    - be protected against military risks such as gunshots, blast, shrapnel and the risk of fire and lightning strike;
    - be protected against natural emergencies phenomenon, such as biological, meteorological and geological;
    - keep the possibility to use fossil fuel if needed with conventional diesel generators;

- be interoperable between allied armies and NATO offering possibility of energy-system data exchanges;
- the technical bricks, systems and sub-systems should be interchangeable either if they come from the same or different suppliers;
- the study should identify a basic energy-system module, in term of power supply, for every deployed camp macro-function (Combat Service, Combat Service Support, HQ, lodging, *etc*.);

o by easily and rapidly transportable (even air-transportable) and deployable solutions:

- without involving a lot of labour force;
- in different geographic and climatic regions from Artic to Tropical regions;
- in different conflict situations;
- under natural disaster conditions;
- housed in container of 20 ISO feet;
- easily deployable and removable.

In order to achieve these requirements, the study should include:

- inventories and identification (benchmark) of the needs of the European Member States taking into account:
  - o the different existing concepts of deployment for overseas operations;
  - o the energy needs according different hypothesis of engagement;
  - o the different technologies, civilian and military, which are developed nowadays to respond to the need of energy self–sufficiency uninterrupted and that could be used for the military forces (including the vital and non-vital systems for the camp);
- regarding Energy storage, Hydrogen/hydrogen-based synthetic fuels are a promising solution. However, in contrast of batteries the possibility and the utility of Hydrogen use (production, transport and logistic, storage and use) in the military context and field operations still need to be confirmed. Proposals should tackle this uncertainty by studying the feasibility of deploying this type of solutions in operational areas particularly in terms of transportation and storage, specifying the hydrogen phases that can be used (such as compressed gas or liquid);
- define an architecture of a modular, lower fossil fuel dependency energy system for a deployable camp. Digital twins, machine learning, and AI could help to define the most efficient architecture and assembled technologies;
- propose tests and validations methods of the possible technology bricks and their integration in a sub-system or system, according to the military requirement;
- all implemented systems will have to comply with cyber-defence and cyber-security requirements.

Expected impact

- Develop cooperation between private enterprises including SME, research institutes and universities in the area of operational energy for defence.
- Adapt civilian sustainable energy technology to military requirements and develop European standards.
- Improve armed forces autonomy, resilience, interoperability and capabilities in operations regarding the growing needs of energy.
- Decrease the total costs of ownership of deployed capacities.
- Enhance the competitiveness and innovation capacity of the EU defence industry in the area of new energies.
- Complete the global European strategy for renewable and sustainable energy, hence tackling the climate change.

2.10.2. Topic EDF-2021-ENERENV-D-NGES: Next generation electrical energy storage for military forward operation bases

Electrical power for Forward Operating Bases has been produced mainly by diesel gensets for decades. Gensets have been seen as a reliable, stable and easy to deploy power source for FOBs and other deployable infrastructure for decades. Nevertheless, a combined momentum for increase of energy consumption during operations, reduction of GHG emissions, concerns about logistical routes safety in long-term international operations and the increase of cost and difficulty of access to fossil fuels lead to a required change of future electrical power supply in FOBs. Considering the technological trends in the energy sector, future FOBs will probably require the use of smart grids combining diesel generators with renewables supported by storage systems.

Specific challenge

The specific challenge of this topic is to assess the current energy storage systems that are developed for civil use and that might be used at a military level. Nevertheless, several factors as lack of European leadership in the technologies, scarcity of resources and geopolitical issues are leading to a European strategy to develop alternative technologies to achieve more sustainable, safer and cost-efficient energy storage systems. In addition, a supplementary effort on these alternative technologies should be made to assure that they are adapted to a deployable, more severe military environment subject to different geographical locations, weather and climate conditions (including extreme environments).

Scope

The proposal must address the development of an application-oriented analysis, including a draft guideline recommendation for novel energy storage technologies is safer and usable for military deployments in forward operation bases; and achieve validation in relevant environment.

Additionally, a set of military requirements (including but not limited to application specific duty-cycles, loading cycles, storage and tactical and environmental conditions) must be collected, aligned and analysed to derive design targets for future energy storage system(s). The proposal will comprehend both components and system integration analysis.

These requirements will then be transferred into a guideline recommendation for the energy storage systems and their integration to be used as a basis for the creation of standards and requirement specifications for procurement procedures. An evaluation of the availability of different energy storage alternatives within the industry and from reliable sources must be made. Additionally, tests of a representative application-specific energy storage system will be carried out for validation of these requirements with the aim to create a European platform for the implementation of these systems.

Targeted activities

The proposals must cover the following activities as referred in Article 10(3) of the EDF Regulation, not excluding possible upstream and downstream activities eligible for development actions if deemed useful to reach the objectives:

- studies, such as feasibility studies to explore the feasibility of new or improved technologies, products, processes, services and solutions;
- the design of a defence product, tangible or intangible component or technology as well as the definition of the technical specifications on which such design has been developed which may include partial tests for risk reduction in an industrial or representative environment.

The proposals must address in particular the following objectives:

Studies:

- analysis of civil-developing novel energy storage technologies and their suitability for deployable, stationary-use applications as FOBs;
- compilation of specific military requirements for energy storage systems from Member States including the energy and power densities, low maintenance and cost comparison;
- review safety requirements, military interoperability issues and operational aspects;
- assess European research, development and industrial capabilities on this area to fulfil future military needs;

Design:

Based on the requirements derived from the feasibility study, and in compliance with them:

- design of a functional technological demonstrator based on the novel energy storage technologies identified, both at component and system level;
- building of the technology demonstrator to de-risk suitable energy storage technologies and their combinations in hybrid systems to achieve functional requirements, including development of advanced software and hardware for power and energy storage

management (like Battery management system – BMS) and validation in relevant environment.

Functional requirements

The proposed solutions should fulfil the following requirements:

General:

- compliance with safety and risk requirements addressing its whole lifecycle;
- compliance with applicable standardisation requirements for energy storage systems design and military interoperability;

Logistics and deployment:

- integration in military standard 20-feet containers;
- the system must be capable of maintaining its performance after long storage time in a military infrastructure, with minimum maintenance and cost levels;
- the system must be safe and ready for transportation on military conditions, including aerial deployment;
- the system must be easily deployable and recoverable;

Operational conditions:

- the system must have high energy density;
- the system must be capable of short charging and discharging cycles while keeping its performance;
- the system must have reduced noise and electromagnetic signatures;
- the system must be capable of performing in severe environmental conditions including use in extreme climatic or sensitive environments;
- the system must have a long lifetime (both in high number of cycles and calendar life);
- the system must be ready for smart hot plug in and out ability of elements and complying with standardization of interfaces for EU Member States;
- the system must present high level of operational autonomy and reduced maintenance.

Expected impact

At strategic level:

- enhance force protection;
- reduce the logistic needs of camps;
- reduce the carbon footprints of military missions and hence tackle the climate change in line with the Union's policies;
- reduce the direct cost of military missions;
- enhance the interoperability of EU Member States' armed forces;

- reduce European dependency on critical raw materials for energy storage systems.

At mission level:

- improve situational awareness, resilience and security of EU operations;
- reduce the logistic needs of camps;
- enable the increase of renewable energy generation in FOBs by maintaining distribution capacity and power quality;
- reduction of hazardous materials from Energy Storage devices components.

2.10.3. Topic EDF-2021-ENERENV-D-PES: Alternative propulsion and energy systems for next generation air combat systems

High value equipment integration in military air platforms contribute drastically to aerial system improvement and innovation. They are key for the European technological sovereignty and strategic autonomy.

Among them sub and supersonic propulsion combined with on-board energy management, within an optimized thrust and power integrated system, will significantly contribute to improve European Air power and to guarantee European aerial superiority.

Specific challenge

The specific challenges of the topic reside in the on-board energy systems coming mainly from the conversion of fuel energy by the engine into propulsion, power, compressed air, *etc*. With the expected increase of power consumption of new airborne equipment (weapons, detection, communication, *etc*.), a global management of energy available on board should now be considered, at a system level, optimizing together propulsive and non-propulsive energies of military platforms (from generation to transport, storage and use). The efficiency of energy use could be greatly improved, as well as the ecological footprint of Defence systems.

Scope

To guarantee a full European technological sovereignty of military air platforms, new technology building blocks of next generation of propulsion and energy integrated systems will be evaluated on a dedicated European Propulsion and Energy ground test platform.

Some of these technologies could also be jointly developed and evaluated on the test platform developed within the frame of this project. Depending on the new technology to be developed and evaluated, one or several demonstrators could be used. Such demonstrators could be for instance engines from several types of aerial platforms: from helicopter engines for new materials evaluation, to fighters' engines for new equipment evaluation.

This platform, open to joint technology development activities, would also be an opportunity for Europe to enhance cross border collaboration between large industrial groups, SME and academics.

Targeted activities

The proposals must cover the following activities as referred in Article 10(3) of the EDF Regulation, not excluding possible upstream and downstream activities eligible for development actions if deemed useful to reach the objectives:

- studies, such as feasibility studies to explore the feasibility of new or improved technologies, products, processes, services and solutions.

Studies: for that purpose, a ground test platform, compatible with the evaluation and/or development of at least the following technology building blocks, must be studied and assessed when relevant:

- advanced fuels (low emission, deoxygenated, *etc*.);
- improved energy generation (propulsive and non-propulsive) technologies to meet increasing electrical demand, including power density considerations;
- improved energy storage technologies (to answer, for example, to the specific needs of airborne directed-energy weapons);
- improved energy distribution technologies, including different network topologies and protection devices (especially for secured communication between local modules and main control system), distributed control system electronics (smart sensors), power electronics (also new semiconductors SiC / GaN) and buffer and interim storage devices (batteries, super capacitors);
- heat/thermal management technologies with integrated power and thermal management (including next generation of heat exchanger);
- instrumentation (development of the test means necessary for the evaluation of next generation of propulsion and energy integrated systems);
- improved propulsion component technologies (*e.g.* bladed rings, nozzle flap, *etc*.);
- new families of materials technologies compatible with requirements for next generation of engines with improved propulsion and energy management efficiency (high temperature materials, capable of operating temperatures within one of these three ranges: 100-400°C, 400-1000°C, and above 1000 °C).

Some evaluations of technologies (see examples listed above) could be jointly performed through this project to identify the relevant ones for maturity upgrading or to support their manufacturing and application processes.

Those evaluations could lead to the development of one or several propulsion and energy ground demonstrators, depending on the type of technology to be evaluated and related demonstrations executions.

Functional requirements

The proposed solutions should fulfil the following requirements:

General

- to enable improving energy efficiency, increasing energy generation (propulsive/non-propulsive) and military air platforms engines performances with complex constraints to reconcile (much higher energy needs/electrical demand of future equipment including armaments and/or sensors, *e.g.* Laser, DEW[55], Electronic Attack/Radar systems, *etc*.) integrated on platforms, future fuels performances and availability (including advanced fuels, *etc*.);
- to explore from off-the-shelf solutions to alternative power/energy generation capacities or innovations and characterize the potential gains, risks, development and production roadmaps regarding military air platforms engines performances needs and roadmaps;
- to consider improvements of the engine systems, from materials to system architectures through components on different levels (including heat/thermal management, energy generation, distribution and storage).

The demonstration solution should be:

- compatible with targeted aerial systems technology needs, in order to allow testing which will identify relevant technologies, ranging from off-the-shelf civilian ones (as long as such civil technologies are not submitted to any control and/or export control from non-European third parties), up to exceeding state-of-the-art military ones. The tests will be conducted in a representative environment, involving existing and emerging flight safety, airworthiness constraints and rules when consistent and in the frame of foreseen demonstration ambition;
- based on a modular architecture enabling an incremental development approach.

The evaluated and/or developed technologies should fulfil the following requirements:

- provide a gain to be characterized for targeted aerial systems (*e.g.* improvement of energy performances, ecological and environmental constraints considerations);
- take into account civilian (pending relevance) and military state-of-the-art to overpass it;
- be compatible with military environments;
- be compatible with relevant national, European and global regulations and standards (*e.g.* REACH[56]);
- be compatible with sustainable EU manufacturing sectors.

[55] Directed-energy weapon.
[56] Registration, Evaluation, Authorisation and Restriction of Chemicals is a European Union regulation dating from 18 December 2006.

Expected impact

- Facilitate the introduction of new aerial propulsion and energy integrated systems technologies through a reduction of their evaluation time and cost.
- Develop EU autonomous industrial sector and enhance cross boarder collaboration (from large industrial group to SME).
- Contribute to European technological sovereignty and strategic autonomy.
- Contribute to improve European air power and to guarantee European aerial superiority.

2.11. Call EDF-2021-MATCOMP-R: Advanced materials and structures, and critical electronics

Proposals are invited against any of the following topics:

- **EDF-2021-MATCOMP-R-PHE:** Materials and structures for enhanced protection in hostile environments;
- **EDF-2021-MATCOMP-R-RF:** Advanced RF components.

Budget

The Union is considering a contribution of up to EUR 40 000 000 to support proposals addressing any of the abovementioned topics and their associated specific challenge, scope, targeted activities and functional requirements.

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

2.11.1. Topic EDF-2021-MATCOMP-R-PHE: Materials and structures for enhanced protection in hostile environments

Specific challenge

Military platforms and military personal protective equipment have to ensure a high level of protection against a large scope of threats and reduce risks of injuries for mounted and dismounted soldiers. This topic is motivated by three long-term challenges:

- new protective systems with the required ballistic protection levels call for substantive investment but after a few years of deployment, the level of protection is most of the time unknown and decisions to discard, redeploy or upgrade, are often taken on uncertain basis or not taken at all. Therefore, the first challenge is to improve proving and certification of durability of current and new materials and protective systems in order to increase the confidence for procurement agencies and industries;
- soldiers are not sufficiently protected against certain threats and new solutions must be developed to reduce the risk of injuries. The second challenge is to find materials, which could protect against new threats;
- the third challenge is to find new concepts of materials, which will be more environmentally friendly, and could reduce EU dependence on certain industries, for instance oil industries. This will ensure Europe’s capability and independence regarding

export control constraints from non-European entities on such critical and strategic materials.

Adequate testing facilities are of utmost importance in all phases of the material and processes development, especially for screening candidate solutions, to generate experimental data (mechanical, thermal, physical, chemical properties, *etc*.). Hence, the design of new test facilities is to be encouraged.

Scope

The topic encompasses research activities on existing materials or new materials or concepts of protection taking into account the specificities listed in the following sections. All types of materials can be considered, for instance: ceramics, polymers, thermoplastics, metals, textiles, hybrid polymer composites, damping materials, nanoparticles and nanocomposites, metamaterials (where the properties of the armour will depend not only on the properties of the material, but also from its structure), *etc*. Considered technologies also include protective systems, non-destructive testing, design methods and tools, numerical modelling and characterization and testing methods. The scope of the topic includes consideration of cost/performances and lifetime/recyclability compromises and the fact that materials and raw materials should as much as possible come from European sources to secure the European supply chain. The establishment of this European industry will require working in parallel on all materials manufacturing stages: raw materials (powder, UHTC, *etc*.), materials manufacturing processes, characterisation of the materials obtained, non-destructive control technology for advanced materials manufacturing. Proposals must also identify elements of a platform to test the outcome of current and future projects in terms of performance and functionality relevant to the activities performed during the project.

Targeted activities

The proposals must cover the following activities as referred in Article 10(3) of the EDF Regulation, not excluding other activities eligible for research actions if deemed useful to reach the objectives:

- activities aiming to create, underpin and improve knowledge, products and technologies, including disruptive technologies, which can achieve significant effects in the area of defence;
- studies, such as feasibility studies to explore the feasibility of new or improved technologies, products, processes, services and solutions.

On the objective of maintaining the ballistic performances when ageing naturally or artificially the proposal must address in particular:

- a study on the state of the art of ageing capabilities of materials or protective systems to identify necessary further development in Europe;
- improvement of knowledge of ageing capabilities of materials or protective systems and their dependence on different environmental and operational conditions;
- study of methods to detect potential failures (non-destructive testing…);

- study of methods to optimize decision to discard, redeploy or upgrade.

On the objective of protection against new threats that are not considered today for vehicles and dismounted soldiers, the proposal must address in particular:

- research activities to improve knowledge, products and technologies of materials or protective systems against novel threats;
- improvement of design methods and tools;
- improvement of numerical modelling and characterization and testing methods;
- study of innovative concepts, new materials, new processes, assemblies or design methodology;
- study to estimate requirements concerning weight/cost and eco-design. The compromises cost/performances and lifetime/recyclability must be addressed.

On the objective of improved materials protecting against current threats the proposal must address in particular:

- research activities to improve knowledge, products or technologies in order to reduce weight and costs of armour and protective systems against standardized threats;
- improvement of numerical modelling and characterization and testing methods;
- study of eco-design capabilities and requirements for future systems (bio-sourced raw materials, recycling…). The compromises cost/performances and lifetime/recyclability must be addressed;
- activities aiming to improve damper technology to increase the dynamic reliability of the frame armour structure.

On the testing platform, the proposal must address:

- study to identify existing services and explore the feasibility of new or improved services to screen candidate solutions and test their protection levels against military requirements and to generate experimental data, taking into account accessibility for new and non-traditional players in the defence sector.

Functional requirements

The proposed materials technologies should fulfil the following requirements:

- withstand ageing (naturally or artificially) while maintaining the ballistic protection performances;
- have reduced weight and cost;
- be compliant with REACH and safety/environmental constraints (eco-design) with as little defence exceptions as possible.

Protective materials against new threats should consider one or more of the following list of threats:

- level 5 to 6 from STANAG 4569;

- laser for protecting equipment inside the vehicle;
- microwaves;
- blast overpressure and fragmentation threat for the dismounted soldier.

Other exploratory threats may potentially be considered. The proposed materials design methods should take into account the final use of the material.

Concerning the protection against new threats and the improved materials protecting against current threats, materials and raw materials should as much as possible come from European sources. The materials manufacturing routes of the proposed technologies must reduce implementation time and costs. Particular attention will be paid to the possibility to produce complex and/or small materials parts, to minimise (or avoid) the machining post-densification, or to assemble different parts.

Expected impact

- Enhance protection of soldiers against current and future threats.
- Optimize life-cycle cost of protective equipment.
- Facilitate the development of new materials and capabilities that a single Member State or individual government or company cannot afford alone.
- Foster an EU autonomous industrial sector.
- Reduce the time and cost for development of protective materials or systems.
- As far as possible, reduce dependency on critical raw materials for the design phase, or use recycling routes for the components/subcomponents.
- Contribute to the strategic autonomy of the EU.
- Contribute to characterization and testing of materials to foster the integration of the outcome of current and future systems into existing systems.

2.11.2. Topic EDF-2021-MATCOMP-R-RF: Advanced RF components

Specific challenge

Gallium Nitride (GaN) technology is a key enabler for high-performance RF electronic components, which are the cornerstone of critical military systems like radar and electronic warfare. GaN has replaced the former Gallium Arsenide (GaAs) technology, providing higher power, bandwidth and linearity to electronic RF amplifiers. GaN technology is deemed strategic for defence systems, and only a few non-European countries worldwide master the whole supply chain needed to provide GaN components for defence applications.

Reducing size, weight, power and cost (SWaP-C) of RF transceiver modules for phased arrays with active electronically scanned arrays (AESA) is essential for radar, electronic warfare and communication systems.

Being aware of the strategic importance of non-restricted access to GaN technology, several European countries started, more than a decade ago, a roadmap for the development of GaN

technology for defence applications in Europe. This roadmap was mainly implemented under the EDA framework. Several projects addressing GaN technology for civil applications received funding under the Horizon 2020 framework. Those activities enabled significant steps towards a European native capacity in GaN. Despite the achieved milestones, further efforts are still needed to develop and consolidate a robust and competitive European supply chain for GaN components.

GaN-based RF transceiver modules are key enablers for modern active electronically scanned array (AESA) antennas, which are one of the essential components of high-end, state-of-the-art military RF systems used for radar or electronic warfare applications. Manufacturing GaN components with shorter gate lengths will allow both for the operation in higher frequency ranges and for shrinking of the transmit/receive modules (TRM), providing adequate RF performance with a high module integration (typically within a lambda/2-spacing). In addition, heterogeneous integration in the same package (SiP, system in package concept) with other technologies (GaAs, BiCMOS, SiGe or CMOS) will extend the functionalities of these modules and meet their SWaP-C requirements.

Scope

There are two key aspects for the building of a GaN supply chain for defence applications in Europe, both of which have been developed in parallel through the aforementioned projects. The first is the accessibility to the material itself (GaN substrates and technologies) and the availability of the processes to manufacture the components (GaN foundries). The second is the capability to design and implement GaN-based solutions (MMIC, *etc*.) for real and demanding defence applications.

Following those two work strands, proposals should address firstly, the need to secure supply of epitaxial wafers with GaN-HEMT structures and the development of an improved GaN manufacturing process.

Secondly, proposals should focus on novel applications in higher frequency bands (Ku, Ka and above, provided these upper bands are progressively enabled by the new GaN manufacturing process) and maturing the applications in the lower microwave bands (pursuing higher bandwidths, TX/RX integration, efficient thermal management, *etc*.).

Proposals should seek complementarity to other former or ongoing projects in other EU programmes and in the EDA framework.

Targeted activities

The proposals must cover the following activities as referred in Article 10(3) of the EDF Regulation:

- activities aiming to increase interoperability and resilience, including secured production and exchange of data, to master critical defence technologies, to strengthen the security of supply or to enable the effective exploitation of results for defence products and technologies;
- studies, such as feasibility studies to explore the feasibility of new or improved technologies, products, processes, services and solutions;

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

The proposed activities should in particular include:

- activities to increase resilience and strengthening the security of supply of European SiC substrate and epitaxy. These are of prime importance to secure the supply chain for GaN military applications;
- improvement of existing processing capabilities and development of new technologies for RF-devices and modules under industrial manufacturing conditions with regard to throughput, yield and costs;
- investigations to gain a deeper understanding of physical effects limiting reliability and device degradation under military relevant operation conditions;
- among the new emerging materials, technologies, processes and tools, the proposed activities can optionally include exploration, in the same study, of benefits of other materials in comparison to GaN on SiC, *e.g.* GaN on Diamond or other suitable substrates, new transistors structures and with shorter gate lengths, improved PDKs, and new methods for measurement and characterization;
- detailed investigation of the appropriate GaN processes for the specific applications and target frequency bands in order to face related challenges in terms of achieving a sufficiently high output power, efficiency, *etc*. within a small device area, especially when moving up in frequency;
- the design, building and testing of GaN MMIC technological demonstrators for different frequency bands and applications with the aim to demonstrate the capacity of the new technologies in terms of power efficiency, linearity and time recovery. Investigation, design and analysis of novel structures and topologies for the MMIC design, in order to fulfil the requirements for high-end defence applications such as but not limited to AESA, EW, robust communication systems, SatCom;
- investigation of new methods for packaging, including low cost plastic packaging and heterogeneous integration of GaN MMICs with other active technologies (BiCMOS, SiGe, CMOS, GaAs) and passive technologies (combiners, circulators, filters) in a same package. This System in Package (SiP) approach will enable a more integrated level for these devices, moving from the concept of TR module to TR channel;
- assessment of Wafer-based Level Packaging (WLP) technology applied to RF sensors SiP;
- development of complements to make the WLP technology compliant with defence specifications for 2D and 3D integration.

Functional requirements

The activities should fulfil the following requirements:

- coverage of a wide frequency range between 100 MHz and 100 GHz (at least from S to Ka band);
- improvement of parameters such as output-power density, power added efficiency, power gain, noise figure and linearity. This could lead to review epitaxy definition and fundamental technology modules (for example gate, ohmic contact, passivation or other…);
- better integration, at integrated circuit level, reducing all factor contributing to losses: for instance number of interconnection levels, low loss passives components, pad size reduction…;
- compliance of GaN technology in regards to fast switching (range of nanoseconds), fast recovery mode in case of intense RF pulse, capability to operate under modulated bias (memory effect), robustness against very high Voltage Swing Wave Ratio, modulated signal for radio usage;
- ability to develop wideband, frequency agile multi-functional RF-modules in order to fulfil different system requirements for radar, electronic warfare and communications (*e.g.* in terms of bandwidth, output power, *etc.*);
- improvement of reliability key figure of merit. This includes the capacity of the technology to sustain a minimum operative temperature of 200°C associated to a Mean Time To Failure (MTTF) compliant of the usage defined by the applications;
- stable performance behaviour versus long operating time;
- robustness against environmental specific conditions (moisture for instance) taking into account integration aspects;
- advanced packaging integration including multi dies integration, moulding encapsulation, power management, extension to millimetre wave, up or down assembly of the elementary dies, internal metallic shielding, mixed analogue to digital heterogeneous integration.

Expected impact

- To progress towards European non-dependence in GaN technology to avoid criticalities about components and electronic ITAR restrictions for defence purpose, increasing EU technological sovereignty.
- To improve the life time of the technologies by power management optimization.
- To deliver circuits meeting the needs of various military platforms: radar, electronic warfare and communications systems for land, marine and airborne applications.
- To improve the competitiveness of European Industries in this strategic technology.
- To be able to deliver to the European Armed forces high-end, state-of-the-art RF military systems non subject to export restrictions.

2.12. Call EDF-2021-AIR-R: Next generation vertical take-off and landing systems

Proposals are invited against the following topic:

- **EDF-2021-AIR-R-NGRT:** Next generation rotorcraft technologies.

Budget

The Union is considering a contribution of up to EUR 40 000 000 to support proposals addressing the abovementioned topic and its associated specific challenge, scope, targeted activities and functional requirements.

Up to one action may be funded under this call.

2.12.1. Topic EDF-2021-AIR-R-NGRT: Next generation rotorcraft technologies

The importance of rotorcrafts, as principal vertical take-off and landing (VTOL) assets/systems, in military operations is widely recognized. Military rotorcraft are the workhorses of battlefields, fulfilling missions like armed reconnaissance, strike, combat search-and-rescue (CSAR), MEDical EVACuation (MEDEVAC), utility, air assault and close aerial support (CAS), which are critical for the success of military operations.

Beyond their pure military role, military helicopters are also key assets for a better civilian security and protection and EU-internal resilience, with critical contribution to disaster relief, civilian search-and-rescue, and sanitary crises.

As such, rotorcrafts bringing the unique ability to take-off and land from almost anywhere, are considered powerful multi-domain operations enablers.

Future combat theatres will mainly take place in congested urban environment – to be expected 65% of population in 2040; moreover most of those congested urban clusters will be in the littoral regions. Thus, potential threats may require moving further away from sea- or land-placed operational bases. Reduced time for intervention will be key, not only to reduce fatalities (faster CAS, MEDEVAC, CSAR…), but also to increase impact of direct actions (faster troop mobility, counter “fait accompli” attempts during hybrid warfare scenario). With major uncertainty on potential 2030+ fields of operations (geographical environment, but also on confrontation intensity), troops may need to operate more swiftly and more autonomously, with VTOL weapon systems offering multiple capabilities for the range of multi-domain (Ground/Air/Naval) missions.

At the same time, advances in systems of systems (SoS) approach, collaborative combat (distributed sensors and functions among collaborative platforms), vehicle and materials features (new helicopter architectures for higher speed and longer range, ballistic protections, signature/detectability reduction) as well as avionics and systems technologies (*e.g.* big data processing, artificial intelligence, next generation and augmented vehicle, more precise sensors) will create major breakthroughs in combat helicopters capabilities.

Capability assessment in EU and NATO frameworks confirms the need to prepare future rotorcraft systems, with hundreds of NATO/EU helicopters to be replaced from 2035 and

beyond 2040. To bundle efforts, the proposals should be consistent with European defence agency and NATO capability working groups.

Specific challenge

To answer this future environment, EU armed forces will require an aligned perspective of the future operating environment (FOE) and research future operating concepts (FOC) of military VTOL-systems including:

- operability and operational flexibility;
- affordability both in procurement and life cycle cost;
- survivability, up to potential Peer nations high intensity conflict;
- sustainability and Operational readiness;
- interoperability for joint and combined operations and collaborative combat;
- resilience, with reduced dependency on critical installation and materials.

Scope

The scope of this topic concerns research on future technologies and the future operating environment (FOE) and future operating concepts (FOC) of military VTOL-systems.

In particular the proposals must address:

- the ends to draw the outlines of the future operating concepts. These outlines are based on the future operating environment (FOE) as well as the role and purpose of VTOL-systems;
- once the outlines are set, the research activities can be focused on the future operating concept (FOC). This conceptual approach concerns all levels of warfare: strategic, operational, tactical and technical. But also logistic and maintenance concepts such as predictive and/or condition-based maintenance, logistical footprint, supply-chain management, acceptable life cycle costs and a flexible/affordable airworthiness certification process with common European (military) certification specifications;
- based on a common perspective on the future (military) operating concept, the required capabilities can be derived, which in turn defines the means: the required military capacities, the required governance to develop and exploit these military capacities and the interoperability requirements. Almost all future military scenarios involve using information to optimize operations. This involves network centric operations in which envisaged future vertical lift obtain information from networks, distribute information on networks and operate closely with other parties to attain intended effects;
- pre-feasibility studies of possible architecture and operational concepts for high performances military VTOL platforms. Those studies will rely on:
    - fundamental work on EU Defence community needs on vertical lift, based on reference combat missions scenarios to be defined, technical and operational studies, concept of operation (CONOPS) definition, battlefield simulations, interactions with advanced vehicle concept designs scalability and applicability to various military missions;

- research on rotorcraft conceptual design: assessment of various vehicle formula scalability and applicability to EU military missions and EU operational requirements. Coordination of technology acquisition efforts to integrate key future capability streams since early concept phase (*e.g.* modularity, survivability, design-to-cost);

- this assessment will include flights with higher speed and longer range VTOL technology demonstrators as necessary, as well as the use of available ground flight simulators. Flying technology demonstrators may be employed to assess new capabilities for military missions, understand key features (*e.g.* manoeuvrability along the flight domain, IR/EM/noise signatures) and potentially as flying test-beds of technologies. First fly-tests, supported by ground flight simulators, should allow EU MoD helicopter specialists to have a pragmatic hands-on insight on the capabilities brought by new high speed / long range / low (reduced) consumption helicopter concepts, when needed for various kind of military missions;
- research on key technologies for next generation VTOL platforms.

This part consists in screening all relevant European technologies available in 5 or 10 years, characterize innovation and technological breakthrough/turnkey challenges fitted to VTOL, and research technological solutions in order to meet future objectives in terms of operability, interoperability, affordability, sustainability and survivability.

Targeted activities

The proposals must cover the following activities as referred in Article 10(3) of the EDF Regulation:

- studies, such as feasibility studies to explore the feasibility of new or improved technologies, products, processes, services and solutions.

The targeted activities must include the initial phases of the concept of operations, operational solutions supported as well as assessing selected technologies, in particular:

- study of the future operating environment (FOE) and the role and purpose of military VTOL-systems in this as SoS;
- study the future operating concept (FOC) including all levels of warfare: strategic, operational, tactical and technical;
- technological support to the evolution of state-of-the-art current helicopter/rotorcraft systems (including EU tilt-rotors and compound rotorcraft). To secure the neutral nature of research in this phase, these widespread studies on potential new systems to come is meant to be in use also for any helicopters/rotorcrafts models associated to European Members States;
- study the required military capacities, the required industrial activities to develop and exploit these military capacities and the interoperability requirements.

Functional requirements

The proposals must fulfil the following functional requirements:

- the study must include a collection and analysis of CONOPS and cost objective complete life-cycle of European armed forces for future rotorcrafts in the 2035/2040+ horizon;
- the study must include an assessment of alternatives between conventional helicopter and different high performance (*i.e.* speed, range/endurance, payload) rotorcraft/VTOL innovative architectures/concepts in terms of operational benefits (*e.g.* long distance deployment, persistence in the area, minimum time-to-target, *etc*.) associated to different types of missions, constraints and impact on cost of operations; it must also propose recommendation and technical solutions to EU armed forces in accordance with operational requirements;
- the study must translate operational requirements into functional challenge, technology calls and conceptual breakthrough;
- the study must carry on preliminary analysis for the foreseen future rotorcraft/VTOL systems. The results may be used also for upgrades;
- the study must conduct research to technology blocks providing performance advantages, in the following domains/areas:
  - situational awareness capability including all-weather and degraded visual environment (DVE) flight, GNSS [57] denied or contested navigation, automated detection, identification and priority ranking of threats, collision avoidance for formation flying between manned/unmanned. All these up to 0/0 in high speed very low level tactical flight and all operations. The study should focus at first on rotorcraft/VTOL specifics, leveraging on potential synergies with other potential projects (about *e.g.* fixed-wing aircraft, drones, and related system technologies);
  - connectivity, SoS, interoperability capability, including combat cloud and MUMT[58] (*e.g.* with air/land/naval manned-unmanned platforms), low drag integration of sensors and antennas. In this context, conceptual evaluation of the feasibility of a SoS design to cope with the challenging features of upcoming and future complex combat/operational scenarios, considering – for instance – a mix of air/land/naval manned/unmanned collaborative/non-collaborative assets, with associated functions and enabling technologies (sensor suites, data management and fusion, cyber protection), should be done;
  - virtual combat mission assistant;
  - enhanced collision avoidance, navigation and control technologies;
  - automated air/air refuelling technologies for rotorcraft;

[57] Global navigation satellite system.
[58] Manned-unmanned teaming.

- survivability capability requirements on architecture and systems, including structural protection (*e.g.* ballistic damage tolerance, impact/crash resistance, *etc*.);
- advanced aero-structures concepts and technologies, taking into account a balanced approach between performances, costs, EU supply chain future resilience, ease of customization and evolution, easier field maintenance, and built-in environmental protection (sand, dust, salt, water, ice...), with test-cases around modular aero-structures with multifunction components;
- self-protection capability;
- low signature/detectability (of various type, *e.g.* acoustic/dB, radar, IR, *etc*.);
- comprehensive assessment of future on-board energy/power requirements, including future vehicle sizing, critical on-board systems (*e.g.* de-icing, directed-energy self-protection and weapons), and related energy/power management possible architectures, definition of key R&T directions (*e.g.* need for high voltage, engine power ratings) and technology recommendations for the EU aeronautic supply chain and research establishments/centres;
- power plant greenhouse gases, fuel/exhaust emission and noise/vibration reduction technologies;
- preparing Technologies accompanying EU rotorcraft engines evolutions (not excluding possible recourse to hybrid propulsion), for improved performances, easier maintenance and optimization of energy efficiency;
- identification of power plant integration supporting technologies (air intakes, nozzles, *etc*.);

- the study must include demonstration of future operating concepts of military VTOL-systems as SoS and vehicle technologies and architecture candidates to ensure enhanced availability, simplified enhanced modularity (including efficient troops-freight payload trade-off and fast reconfiguration), reliability, testability and maintainability to ensure high time of operations and enhanced (life-cycle cost) affordability, also at long term, compared to current helicopters;
- the study must deliver design recommendations on global system architecture to cope with previous systems capabilities but also ensuring affordability, reliability, sustainability and maintainability, with focus on logistics concepts to support operation and maintenance, securing availability of parts and consumables and taking advantage of digital systems for predictive maintenance, digital twins and simulation of user profile;
- the study must support long-term compatibility of EU rotorcraft to future multi-domain and air combat collaborative systems;

- abovementioned capabilities design exploration must encompass potential implementation on brand new and already in-service rotorcrafts. The targeted next generation VTOL systems are thought to be real game-changers on future battlefields. Maintaining the key capabilities provided by VL platforms enabled, in conjunction, by advanced technologies (including SoS related ones), they will boost key operational capabilities such as:
  - safer mission standards for pilots/crew and lower workloads;
  - deeper penetration in enemy territory during complex air assault and special operations, inclusive of littoral/naval missions, and shorter time to reach the spot/enhanced survivability for Close Aerial Support;
  - more effective and faster CSAR/MEDEVAC (also for civilian application/use cases);
  - integration with other defence assets (*e.g.* drones, land/naval forces, *etc*.).

Expected impact

This topic is paving the way for future technology and development programs, leading to:

- prepare 2035/2040+ horizon, building European capabilities for new EU/NATO rotorcraft/VTOL programs, fully compatible to future multi-domain and air combat collaborative systems;
- upgrade existing platforms when possible;
- support the competiveness and excellence of the European industry in this domain and the autonomy of EU in the field of military helicopters;
- increase the efficiency of European Armed Forces;
- increase strategic autonomy and competitiveness of the European defence community (*i.e.* industries and Nations, including academia/governmental R&T/T&E entities), aimed and capable to develop new technologies to be embodied into the future EU/NATO rotorcraft programs.

2.13. Call EDF-2021-AIR-D: Avionics and advanced air combat

Proposals are invited against any of the following topics:

- **EDF-2021-AIR-D-EPE:** Enhanced pilot environment for air combat;
- **EDF-2021-AIR-D-CAC:** European interoperability standard for collaborative air combat.

Budget

The Union is considering a contribution of up to EUR 41 000 000 to support proposals addressing any of the abovementioned topics and their associated specific challenge, scope, targeted activities and functional requirements.

The budget earmarked on 2021 appropriations for this call will be completed by an amount of EUR 109 000 000 from 2022 appropriations. This complement is subject to the adoption of a separate financing decision.

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

2.13.1. Topic EDF-2021-AIR-D-EPE: Enhanced pilot environment for air combat

The future warfare is largely characterised by weapon system automation and networking. While being implemented in all military domains, the concept of swarming and autonomy is in particular evolving in the air domain. Such evolutions have the potential to increase next generation air combat assets effectiveness because connectivity would allow accessing an increased amount of information thus contributing to build a more comprehensive operational picture and UAS assets contributing to the execution of specific mission tasks would multiply the operational impact.

As a result, a large number of actors, effectors, and sensors will be connected, generating an amazing collection of information and data. This induces a great challenge to put the pilots at the centre of missions.

From an air combat pilot perspective, the above evolution progressively adds information for situation awareness building and mission management tasks going beyond the ownship to supervise other platforms under his/her responsibility. The human-in-control principle would imply the risk of information overload or that key aspects of the mission are overlooked.

In order to match the capabilities brought by the above enablers with pilot effectiveness, interfaces need to become more flexible and be able to drive pilot attention to the best course of action. In other words, the cockpit HMI[59], despite the larger amount of information available and the management tasks going beyond the ownship, should evolve to enhance the pilot decision making and action process and timing. Main characteristics would be the capability to delegate under human supervision, an increasing number of tasks to more and more autonomous systems and the capability to adjust to new and unexpected situations that will enable to cut short the cognitive load of operators within a specific framework.

This context will require the development of new sets of equipment and software more and more sophisticated which could take advantage from new technologies like wearable, visionics, haptics, vocal command, virtual operator assistant, augmented reality, 3D holography, implementation concepts, artificial intelligence and autonomy. This will free men from repetitive tasks so they can focus their resources on high value fields of action, thereby improving combat effectiveness.

Specific challenge

From the human-machine relationship point of view, new generation military aircraft inserted in this collaborative air combat will require a new generation of man-machine relationship that allows an ergonomic cooperation between the crew and the machine, a performed effectiveness and a safe flight, as well as the cooperation with other assets, including unmanned ones. The new technologies will allow gaining tactical advantage by assisting the crew as a real co-pilot that answers the crew requests, proposes tactics and procedures and adapts the interfaces to the crew.

[59] Human machine interface.

The definition of a novel design and interaction principles for managing automated/autonomous aircraft functions and cooperating with System-of-Systems team mates, including adaptive interfaces can be defined as man-machine teaming (MMT).

Taking into account the new paradigm, the following subjects could be addressed:

- new or disruptive HMI technologies including for instance displays, wearables, vocal dialog, augmented reality, stereoscopy;
- pilot state monitoring in relation to the mission and systems status;
- services for assisted decision-making support (based on advances techniques like Artificial Intelligence not excluding other approaches).

Scope

Preliminary analyses show that in order to pursue those challenges, the future European aerial combat systems will need to be equipped with an innovative cockpit offering the pilot breakthrough display and interaction capabilities. In this context, it seems clear that new products (head-down, eyes-out, interface modalities, virtual assistant...) have to be developed.

Hence, this topic addresses the rise in maturity, with the objective to reach TRL[60] 4, supported by demonstrations, of technological and technical solutions necessary for future enhanced products.

The proposals may consider existing manned and unmanned air platforms and future ones under development, including training aircraft in a long term perspective or as quick-win.

Against the background of the design of new generation air combat platforms in Europe, or upgrades of those today in service, the following themes have to be considered:

- adaptive human system collaboration: adaptive collaborative HMI for operations in a distributed environment with multiplatform assets and the definition of novel design and interaction principles for managing automated/autonomous aircraft functions and cooperating with System-of-Systems team mates, including adaptive interfaces;
- visualisation: both visualisation products and advanced pilot information presentation capabilities;
- crew monitoring system: systems and techniques able to support and assist pilots, and in general human operators in performing the flight and mission control in a more demanding operational environment;
- interaction modalities: the need for innovative HMI technologies including *e.g.* wearable, visionics, haptics, vocal command, virtual operator assistant, Augmented Reality, 3D holography and implementation concepts;

Emulation of the pilot interactions with its environment might be addressed when needed in a transversal way within the studied areas.

[60] Technology readiness level.

All of those themes will be able to rely, at different levels, on different technology building blocks exploiting the opportunity to use advanced research techniques such as artificial intelligence, machine learning or others that can enable more advanced capabilities for the overall mission performance. This topic is therefore transversal. However, as a complement, it may be interesting to study the theme of "Decision-making system" whose objective would be to prioritize, order and present, whatever the situation during the mission, the most relevant information to the pilot with an objective of efficiency and safety.

Whatever the theme considered, quick wins must be identified, evaluated and tested so as to prepare their implementation on current or upcoming systems.

Targeted activities

The proposals must cover the following activities as referred in Article 10(3) of the EDF Regulation, not excluding upstream and downstream activities eligible for development actions if deemed useful to reach the objectives:

- studies, such as feasibility studies to explore the feasibility of new or improved technologies, products, processes, services and solutions, related to advanced air combat cockpit HMI functions and related technologies enabling effective multi-role and networked operations including MUM-T in a highly contested environment.

In particular, the targeted activities are:

- operational and training use-cases definition to elaborate specifications (performances, safety objectives…). For that purpose, workshops will be implemented with participating Member States and associated countries ministry of defence representatives, including end-users, to establish high-level operational requirements and relevant scenarios;
- for each of the abovementioned themes, relevant technology identification, analysis, including quick wins opportunities identification and analysis leading to the demonstration and development activities dedicated to these opportunities to be performed in a shorter timeframe in order to enable quick implementation process;
- technologies evaluations and demonstrations. These activities will help on to select the relevant technologies to upgrade and to demonstrate further the efficiently of these upgraded technologies through operational scenarios;
- relevant technologies maturation and development.

In order to maximize inter-domain synergies and take advantage of distributed expertise, proposals must address the abovementioned themes according to their following respective description, notwithstanding others fields of interest leading to identify new technologies to be explored, preliminary developed and demonstrated.

Theme N°1: Adaptive human system collaboration

This theme addresses the definition of a new paradigm of human-machine teaming in future collaborative and connected air warfare. New generation military aircraft participating in collaborative air combat will require a human system interface that enhances the awareness of the tactical situation and allows an ergonomic cooperation between crews and machines for a

safe flight and high performance in cooperation with both manned and unmanned assets. This will cover human-machine/human-human/machine-machine Teaming, but will not include functional algorithms.

Legacy human-machine interfaces lack the necessary flexibility and adaptability to meet the demands of future combat systems. To avoid compromising the effectiveness of human operators in the future, applied research is required to address topics such as:

- HMI principles for cross platform mission management considering (human-machine/human-human/machine-machine teaming, not including the specific functional algorithms;
- adaptive HMI mechanisms *e.g.* based on crew management system (CMS) data and in accordance with the specific operational context.

This will then lead to main characteristics of the Human Machine Interface as follows:

- strengthened and adaptive cooperation between all systems, either manned or unmanned, involved in an operation;
- human supervised delegation of tasks to more and more autonomous systems;
- “real co-pilot” like assistance to provide the crew with system proposals and to adapt interfaces.

Theme N°2: Visualisation

This theme addresses both visualization and advanced pilot information presentation capabilities, including 3D presentation, and other novel presentations that could be implemented in the next generation of aircraft, through:

- augmented reality, large area displays (free form, multi touch, auto-stereoscopy), 3D holography and implementation concept;
- helmet mounted display (HMD) solutions crucial for the next generation cockpit. Technological solutions exploration should be carried out for increasing technical characteristics in terms of presentation field and functional capabilities (integrated night vision, primary flight display function, and support for CMS sensors, target designation and view through the cockpit. It will also have to take into account the control of its inertia characteristics (mass and centre of gravity of the HMD carried by the pilot's head).

Therefore, the following areas could be investigated:

- digital integrated night vision;
- HMD wireless link;
- enhanced synthetic vision system (including live virtual constructive visual integration).

Under the scope of this theme, there will be demonstrations with physical, digital mock-up and/or simulations on the basis of operational “use-cases”. An iterative implementation of research findings will be conducted to continuously optimise the performance of the demonstration also based on the initial user requirements.

Theme N°3: Crew monitoring system

This theme concerns the real-time monitoring of the physiological and cognitive states of the crew. The elements of interest, or deleterious capacities, to be monitored are, for example, operator incapacity (G-LoC[61], hypoxia, spatial disorientation...), hypovigilance, attentional tunnelling, mental workload, stress and situational awareness. These aspects are crucial in particular for the future air combat systems where the operational environment and the way of operate are significantly more complex than the current ones. Crew monitoring system can be applied to operational embedded systems as well as to training systems (embedded or on ground).

In order to more specifically mature the CMS models the following areas could be investigated:

- mental workload;
- ability to collaborate;
- situational awareness;
- stress.

The validation of CMS models is a crucial point in the CMS chain's rise to maturity also based on a pilot behavioural knowledge base (PBKB) that needs to be contextualised in accordance to the diversity of human, missions and tasks, including through AI- and ML-based techniques.

Under the scope of this theme, there will be demonstrations with physical, digital mock-up and/or simulations on the basis of operational use-cases. An iterative implementation of research findings will be conducted to continuously optimise the performance of the demonstration.

Theme N°4: Interaction modalities

This theme addresses both the modalities of interaction as well as their combination in the field of *e.g.* wearable, visionics, haptics, vocal command, touch, gesture, *etc*.

In terms of means, it takes into account:

- audio, in terms of input/outputs: voice command, natural language processing, in a very constrained environment such as that of a fighter, voice synthesis and advanced audio functions such as 3D Sound for example;
- eye: the eye tracker which is used as a CMS sensor is here dedicated to interaction. Coupled with another modality such as voice, it is a vector of efficiency for target designation in an eyes-in or eyes-out use;
- touch: a particular objective will be to study multi-touch (up to 5 fingers) technologies to interact with the displays;
- gesture controls;

[61] G-force induced loss of consciousness.

- haptic/tactile display of information;
- handwriting recognition and more generally the ability to interact naturally with a "white board".

Multimodality would provide greater security, resilience and accuracy by removing ambiguity about the operator's intentions.

Under the scope of this theme, there will be demonstrations with physical/digital mock-up and/or simulations on the basis of operational use-cases. An iterative implementation of research findings will be conducted to continuously optimise the performance of the demonstration.

Functional requirements

The proposals must fulfil the following requirements:

(1) in order to support the future air collaborative combat:

- take into account the new paradigm of human-machine teaming in the future collaborative and connected air warfare and adaptive cooperation between all systems, either manned or unmanned, involved in multi-assets operation:
  - through a strengthened and adaptive cooperation between all systems, either manned or unmanned, involved in an operation;
  - based on a human-supervised delegation of tasks leading to more and more autonomous systems;
  - using a “real co-pilot”-like assistance providing the crew with system proposals,
  - piloting performance monitoring for adaptive HMI;

(2) in order to improve human-machine performances:

- human-machine performance must be evaluated according to different criteria to be defined in the proposals;
- human factor aspects must be taken into account to develop the technologies (especially physical and cognitive ergonomics);
- physical ergonomics must take into account the anthropometrics data considered for the air combat domain;

(3) the proposals must comply with the following specific technical requirements:

- the technologies have to be scalable for existing fighters or future fighters in order to apply the “quick-win” principle;
- each technological building and capability blocks must be evaluated and demonstrated through physical or digital mock-ups and simulations based on the studied “use-cases” scope;

(4) the proposals must ensure that the treatments of data collection about humans to build models or algorithms are compliant with the European GDPR (General Data Protection Regulation) rulemaking.

Expected impact

- European platforms for enhanced combat pilot technologies tests and demonstrations to welcome joint or national tests and demonstration needs.
- Consolidation of a sector of excellence in Europe for enhanced combat pilot based on innovative technologies.
- Generation of inputs for the mid-term and long-term development of next generation air combat cockpit HMI.
- Definition and "demonstrator development" of novel cockpit HMI technologies.
- Increase mission capability, efficiency, effectiveness and performance in air combat missions (more safe for pilot and limiting the collateral damage) exploiting the emerging technologies.
- Provision of a potential starting point for developing EU guidelines in the frame of advanced HMI design for managing systems-of-systems operations.
- Provision of an opportunity for cross-ministries of defence and cross-industries exchanges in the subject of cockpit design and pilot operating procedures.
- Strengthen European industry in advanced air combat cockpit technologies independent of third countries.
- Quick wins identification to be implemented on current or upcoming systems.

2.13.2. Topic EDF-2021-AIR-D-CAC: European interoperability standard for collaborative air combat

European air forces share the aim to have highly integrated multiplatform mission management capabilities:

- to enable the variety of different assets, manned and unmanned, to operate during an air operation together jointly and synchronized (including interoperability with NATO, and potentially other coalition situations);
- to share efficiently sensors and effectors resources of manned and unmanned assets;
- to share data and information (*e.g.* situational awareness), leading to informational and ultimately decisional superiority.

These capabilities objectives imply the deployment of connected collaborative combat which endorses the fact that the systems ensure several properties: to ensure the interoperability of heterogeneous systems (different types of aircraft for example), to enable secure and standardised exchanges of data and resources, to easily incorporate changes in mission system software to take into account operational needs (modification of existing functions, tactical needs, evolutions of rules of engagement, add on of new functions…).

To satisfy those challenges at the level of European air combat, design rules, compliant with existing standards when needed, and applicable standards definition to future mission and collaborative air combat systems or to evolution (new functionalities) of the existing mission systems have to be defined in the European industry landscape on the basis of operational realities and user requirements.

The need and relevance of those standards has to be concretely demonstrated through focused end-to-end connections as well as the seamless integration of a maximum of allied weapon systems to a networking environment and their interaction, thus illustrating all the benefits of advanced collaborative combat. This will pave the way for future European collaboration at the operational level with improved capabilities.

Specific challenge

The key challenge is to jointly build a European perspective enabling the Member States to address at middle and long term collaborative air combat capabilities combining future air combat systems, manned or unmanned platforms, legacy platforms and their evolution, including sensors and effectors. Nowadays, European air forces are built on a wide variety of heterogeneous systems. This variety brings the challenge of interoperability on the functional, software and hardware levels. With the plausible introduction of unmanned systems into air combat, future interoperability requires a far deeper interconnectedness that can be provided with new generation of tactical data links.

This implies the development of interoperability standards enabling collaborative combat to provide for a common entry point of proprietarily developed systems. These standards would address IT evolutions (communication, dissemination, services sharing, cybersecurity) and take them to the next level, with all participants agreeing to the related details.

Different mission systems on board different Nations' assets would benefit from a service-oriented architecture among them. This approach enables all Nations to operate as a whole without the need to use the exact same equipment or assets. It indeed specifies the functional interfaces between assets without imposing specific systems within those assets. The definition of such a service-oriented architecture and its relying standards is a key milestone for modernization of the capabilities of EU military fleets.

Another effort axis consists in studying, as a consistent system approach, the integration of platforms and effectors.

Edge-computing on board new generation manned or unmanned assets can bring new capabilities, relying on mission computers with vast amounts of processing power, storing capacities. On their basis, several mission management functions can be implemented or improved, like the closely integrated operation of manned and unmanned assets through collaborative mission management or smart processing of heterogeneous sensor data (radar, optronics and electronic warfare) across heterogeneous assets. Equally, formation, communication, information or weapon management can be revolutionized, even for legacy systems. Mission management and sensors collaboration improvements allow for an overall better operational performance of each asset and a better perception of their tactical environment. Scalability of those mission computers would be a key element as well.

An optimized usage of resources in the combat air domain would facilitate the increase of mission effectiveness. In such more cooperative environment, standards and common way of sharing information among assets are necessary, with impact on the way to design mission system functions. To enable those capabilities, the definition of data formats – a common referential – for those applications is necessary for the nations, as well as common processes to share them – common languages.

This implies also to address the evolutivity of the mission systems to enable adaptation to new tactics, concepts and collaboration standards, definition of design rules applicable to legacy systems evolution and futures systems. This will lead to exploit key technologies such as artificial intelligence for instance to enable some collaborative services among air platform. Existing and futures open standards (*e.g.* like ECOA[62], IMA …) need to be addressed to cope with the challenge of harmonizing the software footprint of all kind of equipment on board military aircrafts and could be a good starting point.

More specifically, the command and control of manned and unmanned systems from an airborne combat asset perspective, as well as the handling and exploiting of the wealth of information generated by distributed sensors across collaborating assets, will require the application of dedicated AI technologies in a variety of technical and operational domains. Making sure this "digital partner" outputs are trustable and do not jeopardize the human responsibility in military action is paramount. In this regard, identified AI work streams could include (without being limited to) with a specific focus on airborne combat asset use cases:

- flight certification and airworthiness issues with AI-based functions on board;
- identification, selection and usage prototyping of engineering tools and methods enabling the sovereign use of protected AI Data and algorithm libraries.

This topic also has to take into account relevant outputs and results of ongoing and potential future European projects (for example, but not limited to: EDIDP, EDF, multilateral projects…), as well as future combat programmes, and pursue a maximum level of compatibility, compliance and interoperability.

Scope

The scope of this topic is to propose solutions supported by demonstrations when relevant on the major axis presented above, thus providing air collaborative combat standardised solutions, mission systems evolutivity, standardised effectors interfaces and European sovereignty over AI technologies (tools, methods and libraries).

The targets are twofold: first, medium-term outputs to be implemented as standardised collaborative mission management enhancements for existing or upcoming European operated platforms, on the basis of commonly agreed standards and requirements of the participating Nations to favourably influence the construction of future European air combat capabilities. Potential implementations on existing platforms are not part of this project but are likely to be

[62] European Component Oriented Architecture.

specified based on developed standards for an implementation in the respective national perimeter.

The proposals must consider manned and unmanned combat platform assets/concepts operated by the participating Member States, from current or upcoming ones to future air combat systems in Europe within an interoperability incremental approach. Future air combat scenarios require to rethink collaboration which is inseparable from an extended interaction between combat aircraft and a diversity of collaborative assets contributing to air combat operations also interfacing with any other domain (air, land, sea, space, cyber, …) (*e.g.* mission aircraft, tanker, JTAC…). This includes the need to consider interoperability with system of non-EU origin, to provide for compliance with NATO and other coalition situations, to be identified through the high-level operational requirements definition.

The proposals must consider scenarios for air combat operations in contested and highly contested environments at least geographically located in geographic Europe, Northern Africa and Middle-East. This could be complemented (*e.g.* Air defence and air policing within European airspace) when the common high-level operational requirements will be set up in close alignment with participating Member States' representatives.

Targeted activities

The proposals must cover the following activities as referred in Article 10(3) of the EDF Regulation, not excluding possible upstream activities eligible for development actions if deemed useful to reach the objectives:

- studies, such as feasibility studies to explore the feasibility of new or improved technologies, products, processes, services and solutions;
- the design of a defence product, tangible or intangible component or technology as well as the definition of the technical specifications on which such design has been developed which may include partial tests for risk reduction in an industrial or representative environment.

In particular, the targeted activities must include:

(1) Air Collaborative Combat: interoperability of heterogeneous systems

- development of use-cases, high-level operational requirements with end-users to support the consolidation of a common operational perspective with regard to Air collaborative warfare for EU capabilities, manned and unmanned;
- functional architecture and technical architectures principles of airborne combat asset mission systems for standardisation and interoperability scope;
- definition of required Interoperability standards for mid- and long-term platforms from existing aircrafts manned or unmanned to the new generation of platforms, communications, security, data/services: analysis of existing and emerging standards, gap analysis, existing standards evolution or new ones;
- definition of standards for Services Oriented sensors interfaces: analysis of existing and emerging standards, gap analysis, existing standards evolution or new ones;

- machine to machine collaboration (architecture principles for interoperability of heterogeneous assets, definition of information transfer protocols);
- human - system collaboration (socio-technical aspects): impact of AI implementation in military assets, operational (SA and decision making, effects delivery), ethical and regulatory aspects;
- demonstrations (Proofs of Concepts through simulations, ground/flight demos…), implementation of existing and envisaged standards on ground and/or demo platforms, illustrating concrete benefits of collaboration between connected assets taking part in an air operation. This could be envisaged on existing platforms.

In a transversal way, activities must be lead with attention paid to:

- identification of quick wins, based on existing EU technologies, open standards and initiatives, taking into account operational, technical and legal boundaries and limitations, and national specifics, *etc*.;
- cyber resilience aspects and data protection.

(2) Air collaborative combat and mission system evolutivity: Software development standardisation and hardware reference model development

- dissemination and development/enhancement of existing or new standards for software development (*e.g.* ECOA, IMA …): advanced IT technologies should bring a significant advantage for the mission system development and improvement of the mission system capabilities;
- open-based component oriented architecture is seen as a good candidate to reduce through-life cost and timescales for production and updates of complex integrated system such as an airborne Mission System. Existing standards will be analysed taking into consideration the specific needs. Certifiable plug and play, state-of-the-art system update, self-healing databases mechanisms have to be investigated;
- tools for supporting the standard definition should be identified and developed if needed;
- development of references of a hardware model: common architecture principles and standardisation of computer interfaces.

(3) Effectors integration on airborne platforms

Future airborne systems will show a deeper integration of platforms and effectors (dataflow, energy supplying…) to answer to operational needs (reactivity, safety, flexibility, LO demands …). Starting from the existing effectors functions, the study aims at identifying integration strategies between the future portfolios of effectors and aerial platforms at the turn of 2030 and beyond. Existing and future standardisation trends will be analysed and considered in the proposal of integration strategies. As other projects are ongoing (*i.e.* LSIF), the study will focus on add-on to the current standards to take into account new functionalities required by smart weapons (expendable RC,

networked armament…) and extended operational aspects in addition to physical interface.

(4) AI Technologies

- formalisation of airworthiness and safety typical issues related to AI-based functions on board;
- identification, selection and usage prototyping of AI toolkits (*e.g.* European alternative to tools like Tenserflow, Pytorch or RLlib), libraries, methods (*e.g.* machine learning, neural networks, …) enabling an independent and sovereign use of these technologies by the EU for military purpose Definition at European level, of methods and processes for military qualification of non-safety critical and trustable AI functions;
- demonstration (proof of concept) of tools and processes for the development, certification and validation of "trustable" AI driven operational services (*e.g.* dynamic tasking of assets, decision-making support, data routing processes) for the purpose of validating feasibility and airworthiness/safety issues.

Those activities will be complementary of other studies on AI technologies (*e.g.* dealing with concerns as Frugal and Robust learning for rapid adaptation of AI systems) having a specific focus on airborne use-cases.

Functional requirements

The collaborative air combat capability must fulfil the following requirements:

(1) The collaborative air combat must improve the interoperability of heterogeneous aerial systems (from existing aircrafts to the new generation of platforms, manned or unmanned), including when in coalition situations with European and NATO forces.

This improvement must be based on the analysis of existing and emerging standards, promotion/evolution of existing standards or development of new standards as well as results of relevant ongoing projects and future combat programmes.

The standards must be applicable for the design of next generation combat assets mission system (new generation fighter, unmanned combat asset) and the upgrades of legacy combat aircraft.

The standards definition activities must cover the following perimeter:

- in order to support collaborative mission management and sensors collaboration between heterogeneous assets:
  - functional and technical architectures principles;
  - functional services oriented interfaces principles;
  - services oriented architectures and functional services oriented interfaces for mission system;
  - services oriented sensors interfaces;

- in order to enable interoperability, secure exchange of resources/information and data sharing with others assets in various coalition situations (NATO, EU and non-EU, national context) while offering a better evolutivity and interchangeability (S/W and H/W level):
  - communications architecture principles (including cyber issues);
  - functional interfaces of the different layers of communications architecture (Core Services and Communications Services according to C3 taxonomy);
  - validation methods and associated means (*e.g.* functional simulators);
- in order to improve interoperability and development efforts of effectors:
  - functional and physical interfaces of future effectors (remote carriers and weapons);
- in order to improve mission system scalability and the associated development efforts (easier and faster aerial mission systems development and upgrade):
  - software development;
  - development of hardware references.

(2) The collaborative air combat should participate to structure and develop a European ecosystem to support AI technology sovereignty for military usages.

For this purpose, the activities must cover the following perimeter:

- formalisation of airworthiness and safety typical issues related to AI-based functions on board;
- identification, selection and usage prototyping of AI toolkits, libraries, methods enabling an independent and sovereign use of these technologies by the EU for military purpose;
- definition of harmonized methods and process at European level for military qualification and certification of AI-based functions;
- validation of feasibility and airworthiness/safety issues through demonstrations (proof of concept) of tools and processes for the development, certification and validation of "trustable" AI driven operational services (*e.g.* dynamic tasking of assets, decision-making support, data routing processes).

Expected impact

- Shared consolidated European perspective for collaborative air warfare.
- Incremental increase of the interoperability of warfare systems – current and future – so that the participating Member States' armed forces would be able to "plug and fight" in order to operate collectively and efficiently.
- Better usage of resources (single and multiple domains and assets).

- Quick wins identification to be implemented on current or upcoming systems (*e.g.* ability to associate different generations of assets, dissemination of conception guidance for long-term development of future European air combat system). Quick wins approach would also enable cross-border SMEs to participate in this topic.
- Common European standards for Member States.
- Harmonization of European industrial processes and methods for the development of assets or equipment contributing to collaborative air combat capabilities.

2.14. Call EDF-2021-AIRDEF-D: Protection against high velocity aerial threats

Proposals are invited against the following topic:

- **EDF-2021-AIRDEF-D-EATMI:** Endo-atmospheric interceptor – concept phase.

Budget

The Union is considering a contribution of up to EUR 28 000 000 to support proposals addressing the abovementioned topic and its associated specific challenge, scope, targeted activities and functional requirements.

The budget earmarked on 2021 appropriations for this call will be completed by an amount EUR 72 000 000 from 2022 appropriations. This complement is subject to the adoption of a separate financing decision.

Up to one action may be funded under this call.

2.14.1. Topic EDF-2021-AIRDEF-D-EATMI: Endo-atmospheric interceptor – concept phase

Air Superiority is one of the eleven EU capability development priorities identified as part of the revised 2018 capability development plan. This priority includes specifically A2AD type (anti-access area denial) and BMD (ballistic missile defence) capability shortfalls. The emergence of new threats such as manoeuvring ballistic missiles and hypersonic cruise missiles (including air launched ones) or hypersonic glide vehicles represents an additional challenge for European and NATO ground and naval-based air defence systems. Existing knowledge and technologies in the field of weapon systems and missiles design inside the EU represent however an opportunity to explore the feasibility of an endo-atmospheric air defence effector able to intercept current and emerging post-2030 ballistic and cruise missile threats.

Specific challenge

This topic is an opportunity for Europe to federate efforts under a European design authority to master critical technologies, materials, components and expertise key to develop a state-of-the-art endo-atmospheric interceptor. The concept exploration study of the interceptor will be

the cornerstone for possible future European ground and sea-based missile defence systems, able to complement significantly and improve the robustness of NATO BMD and TBMD[63].

Scope

The proposals must address surface-to-air interceptor solutions including interceptor concepts studies, and associated early maturation activities, until an interceptor mission definition review (MDR) and a preliminary requirements review (PRR) approved by the cooperating Member States. The proposals must aim to provide two main results:

(1) the selection of an interceptor solution to counter the post-2030 theatre air and ballistic threat;

(2) the initial maturation of the most critical related technologies.

Targeted activities

The proposals must cover the following activities as referred in Article 10(3) of the EDF Regulation, not excluding upstream and downstream activities eligible for development actions if deemed useful to reach the objectives:

- studies, such as feasibility studies to explore the feasibility of new or improved technologies, products, processes, services and solutions.

In particular, the proposals must address:

- **the iterative definition of interceptor detailed requirements**, based on:
  - the definition with cooperating Member States of a set of missions, threats, attack scenarios including salvos or combined attack, and user requirements, the definition of a workable concept of operations (CONOPS), including interceptor association with external lower/upper layer effectors and early warning sensors;
  - the detailed characterization of the relevant threats to be addressed by the future interceptor;
  - the selection with cooperating MS of relevant weapon systems (WS), platforms and command and control (C2) architectures to be considered for the interceptor concept and development activities, in consistency with Member States roadmaps for these elements at the horizon 2035+. Considering the early stage of the interceptor activities, the proposals will favour generic/high-level WS, platform and C2 assumptions;
  - the selection with cooperating Member States and characterization of the relevant sensor suites, including fire control radar and early warning sensors, to be considered for the interceptor concept and development activities, in consistency with Member States roadmaps for these elements at the horizon 2035+, and with Member States' activities related to space-based early warning. Considering the early stage of the interceptor activities, the proposals will favour generic sensors models, taking into account existing technology and main planned evolutions in the considered horizon;

[63] Theatre Ballistic Missile Defence.

- the elements coming from concept exploration studies;

- **the concept exploration studies and performance assessment for possible interceptor solutions,** notably regarding:
  - the definition and assessment of the candidate interceptor physical architectures;
  - the definition and assessment of the candidate interceptor functional architectures, including integration within the relevant WS;
  - the assessment of interceptor and global WS performances, in behavioural and accurate (6-DoF[64]) simulations combining physical and functional accurate modelling for the candidate interceptor solutions. In particular, the assessment will include detailed simulations of the main interceptor flight phases, and will take into account generic radar models to estimate the probability of interception against each type of threats for the selected interceptions points;
  - the physical and functional integration aspects of the candidate interceptor concepts on the relevant platforms and launchers identified with the Member States, including safety aspects;
  - the munition management aspects during its complete lifecycle, including transportability, integration to different platforms launchers, safety and integrated logistic support;
  - the testing facilities, for development and qualification;
  - the trainings aspects, including firing tests;
  - the economical (non-recurring and recurring costs) and general risk analysis of candidate concepts;
  - the proposal for a best concept candidate for further maturation and preliminary design phase, based on complete value analysis including performance, costs, risk, modularity, manufacturability, safety, consistency with Member States operational needs, current/planned platform sensors and lower layer interception means, with jointly defined detailed criteria and hypothesis;
  - the mission definition review (MDR) and a preliminary requirements review (PRR);
- **the early maturation activities key for developing an endo-atmospheric interceptor,** including best suitable propulsion solutions for boost phase, midcourse phase and endgame, notably:
  - activities related to main interceptor functional segments, in consistency/support with functional requirements and concept exploration activities;
  - activities related to interceptor technologies and equipment, in consistency/support with the functional requirements and the concept exploration activities);

[64] Degrees of freedom.

- the maturation level raised through the present concept phase must be sufficient to allow the most critical technologies and equipment to reach TRL 6 within 3 years, by means of the possible following assessment phase which has to be consistent with the scope of the retained concept;
- identification of complementary maturation plan allowing to reach TRL 6 for most critical technologies and equipment.

Functional requirements

Proposals must fulfil the following requirements:

- the candidate interceptor solutions must operate with both naval and ground systems;
- the candidate interceptor solutions must operate with platforms that are consistent with the Member States' roadmap at the horizon 2035+ for European navies and ground systems;
- the candidate interceptor solutions must operate with WS architectures and sensor suites that are consistent with the Member States' roadmap at the horizon 2035, including potential space-based early warning system against ballistic and hypersonic missiles;
- the candidate interceptor solutions must provide collaborative engagement capabilities (CEC) at missile level and be compliant with CEC at system level (*e.g.* LOR[65], EOR[66]) to allow engagements in a multi-system and multi-platform architecture);
- the candidate interceptor solutions must address as a priority following high-level threat set:
  - BM[67] up to 3500 km of range, including those with the ability to significantly modify the atmospheric part of their trajectory;
  - ASBM[68] up to 2500 km of range;
  - hypersonic glide vehicles released by TBM[69] up to 3500 km of range;
  - high altitude hypersonic and supersonic cruise missiles;
- the candidate interceptor solutions must enable self-defence, force protection and area defence against the high level threat set;
- depending on possible complementarity with other Member States weapon systems, the candidate interceptor solutions should address performance against the following threat set, keeping in mind that the primary design optimization must aimed at the high-level threat set mentioned above:
  - sub- and super-sonic cruise missiles;
  - air breathing targets (fighter, aircrafts, UCAV[70], HALE[71]…);

[65] Launch on remote.
[66] Engage on remote.
[67] Ballistic missile.
[68] Anti-ship ballistic missile.
[69] Theatre ballistic missile.

- sub- and super-sonic sea-skimming missiles;
- other high manoeuvring missiles;

- WS assessment and candidate interceptor concepts sizing must consider following elements for the generic sensor suites:
  - performances achievable by the other Member States' activities and/or EU-funded activities (*e.g.* through the European defence industry development programme) regarding space-based early warning;
  - key ground-radar requirements, considering technologies upgrade in the radar domain in the 2030+ horizon and relevant frequency bands, and associate a "risk level";
  - provide the generic models and the key sensor suite characteristics to represent the sensor suite for the WS and effector concept(s) assessment;
- following aspects for the abovementioned threats must be characterized:
  - mission and operational CONOPS;
  - flight phases and associated kinematic characteristics;
  - physical characteristics and observability (detectability: signatures in infrared (IR) and radio frequency (RF) bands, plasma effects);
  - trajectory constraints due to guidance means (active/passive/semi-active seekers, IMU[72], GNSS[73], …), to physical integrity (thermal load, …), and terminal accuracy (miss-distance, CEP[74]);
  - manoeuvrability and penetration aid (PENAIDS) devices and/or tactics;
  - generic model for each type of threats;
  - vulnerability and functional / physical destruction criteria;
  - potential users and temporal horizon;
  - possible threats evolutions (2040+ horizon);
- interception performances requirements (interception altitude, range, hit probability, lethality …) must be detailed for each selected threat considering possible threat behaviour (manoeuvres, countermeasures), assets/areas to be defended and combined attacks scenarios;
- interceptor concepts must be sufficiently developed at individual stages as well as complete munition level to assess the feasibility of a single interceptor or a family of interceptor, and to provide specifications and steering for the specific technology, equipment and functional chain maturation topics;

[70] Unmanned combat aerial vehicle.
[71] High altitude long endurance.
[72] Inertial measurement unit.
[73] Global navigation satellite system.
[74] Complex Event Processing.

- the studies and initial de-risking activities, including technology/sub-systems demonstration when appropriate, must be included for the following technologies and equipment:
  - high-temperature materials and structures;
  - high-supersonic airframe and thermal management;
  - advanced guidance and control system;
  - high-temperature and very-high performance fins actuation system;
  - solid propulsion and thrust vectoring devices (small to large motor calibres);
  - high-supersonic ramjet (midcourse) propulsion;
  - IR sensor(s), to address the game changing emerging threats (hypersonic cruise missiles, fast ASBMs/TBMs, hypersonic gliders), including sensor window and cover if necessary;
  - RF sensor(s), to operate at all altitudes, but with a more modest level of ambition against the above mentioned game-changing threats, including covers/radomes;
  - pyrotechnic divert and/or attitude control systems;
  - warhead, and warhead triggering sensors;
  - long-range, high rate and low latency datalink system, including compatibility with existing datalink systems;
- the studies and initial de-risking activities, including functional segment demonstration when appropriate, must be included for the following functional segments:
  - interceptor integration to ground and naval platform, including hanged-fire safety case;
  - midcourse aero-propulsion and controllability of high-supersonic ramjet-based airframes;
  - stages separation and shroud ejection in supersonic regime;
  - threat discrimination, classification and identification;
  - tracking and prediction of possible flight paths for fast and manoeuvrable threats;
  - engagement planning, mid-course trajectory optimization and guidance against fast, manoeuvrable threat, even with non-predictable future behaviour;
  - multi-mode high-altitude terminal control architectures, and advanced guidance (hit-to-kill) for endgame (IR and RF);
  - high-end threat acquisition and tracking with terminal sensor;
  - enhanced lethality against new high-end threat, including aim-point selection and warhead triggering.

Expected impact

- Contribution to the defence and security interests of the EU and its Member States:
  - contribution to the EU strategic autonomy level of ambition, as defined in the CDP, in particular regarding Air Superiority;
  - increased resilience enhanced protection of critical assets and improved force protection of ground and naval units against post-2030 threats;
  - complementarity between EU and NATO by reinforcing the qualitative and quantitative contribution of the European allies to the NATO missions, in particular the BMD mission.
- Contribution to enhanced interoperability between armed forces of the Member States, stimulation of European doctrine and European standards.
- Contribution to Europe's resilience and European technological sovereignty:
  - contribution to the industrial autonomy and technological sovereignty through the development of concepts, critical functional chains and equipment under a European design authority;
  - contribution to innovation through the investigation of new and disruptive technologies and concepts;
  - support to the European missile systems ecosystem in the long-term and pull up technologies to be reusable in other missile segments (guidance chain, seeker, propulsion, materials…);
  - contribution to strengthening the competitiveness of the EDTIB (European defence technological and industrial base) by creating new market opportunities;
  - contribution to relocate some technologies and expertise, materials and components in Europe under a European design authority in line with the EU industrial autonomy and technological sovereignty ambitions.

2.15. Call EDF-2021-GROUND-R: Precision Strike Capabilities

Proposals are invited against the following topic:

- **EDF-2021-GROUND-R-IW:** Improved warheads.

Budget

The Union is considering a contribution of up to EUR 10 000 000 to support proposals addressing the abovementioned topic and its associated specific challenge, scope, targeted activities and functional requirements.

Up to one action may be funded under this call.

2.15.1. Topic EDF-2021-GROUND-R-IW: Improved warheads

Defeating improved protection systems of main combat platforms, hardened targets and reinforced (critical) infrastructures remains a focal challenge for military operations. Enhanced effects on targets, like blast, perforation, penetration, shock, bubble effects or electromagnetic pulse, are required to defeat such advanced protection systems. In this way, the development of new types of warheads with higher performance is required. Activities should cover the research on an enhanced penetration performance.

Specific challenge

In recent years, new threats have emerged on the battlefield. Among these threats are next generation main battle tanks. These systems apply active protection systems (APS) that render conventional anti-tank weapons ineffective. However, warheads with a standoff capability, which can be initiated outside the range of an APS, might destroy such targets. In addition, explosive reactive armour (ERA) and passive armour were improved during the last years. In this respect, enhanced shaped charge technologies are required.

In recent years, there has also been a steady increase in urban warfare. Thus, battlefield engagements are not limited against main battle tanks or fighting vehicles, but increasingly against infrastructure. Often, these infrastructures apply high-performance concrete, which makes engagements more challenging. Consequently, it necessary to obtain small calibre penetrator warheads for battlefield weapon systems that can be effectively employed against infrastructure. In this respect, new penetrator technologies are required.

Scope

The scope of the research action should be:

- research on technology of explosives: development of a technology of production of explosives charges with high homogeneity (uniform density distribution in the entire volume of the charge), geometric accuracy and high detonation parameters;
- research on technology of liners of shaped charges and explosively formed projectiles (EFPs);
- development of a technology of production of precise liners made of conventional materials (copper, Armco iron) with high structural homogeneity, chemical purity, *etc.*;
- development of a technology of production of precise liners made of new materials, *e.g.* manufactured with the use of additive techniques; with a programmed texture affecting the projectile formation process in such a way that the final shape of the projectile improves its stabilization on the flight path; slow stretching shaped charges allowing to keep its integrity as long as possible;
- optimization of the shapes of the liners;
- development of a technology of manufacturing of the warhead shells providing high strength, accuracy and repeatability of assembly, maximizing the penetration capability of the warheads and minimizing the weight of the entire system; *e.g.* by using a steel-

composite shells with circumferential reinforcements made of carbon or glass fibres in a polymer matrix;

- development of new methods of explosive initiation, ensuring additional acceleration and appropriate shape of the detonation wave, axisymmetric deformation of the liner and, as a result, maximization of its penetration capability;
- development of multi-liner warheads (one explosive charge form and accelerate several projectiles). Such solutions will enable defeating armoured vehicles, but also can be used to destroy various types of infrastructure during military operations in urban areas (small calibre/low mass of explosive limit the negative side effects of detonation of the EFP, *e.g.* damage of buildings);
- development of initial concepts of new warhead carriers as well as selection of existing ones and definition of new warhead applications related to their structures (grenades, mines, drones, *etc.*);
- definition of numerical models of the warhead/target systems and performing computer simulations in order to initially evaluate the penetration capability of newly developed warheads;
- performing experimental tests determining the functioning of the developed warhead systems.

Furthermore, the proposal must address penetrator warheads that can be effectively employed against infrastructure. Moreover, the proposal can address other technologies that offer added value in the context of next generation battlefield targets.

Targeted activities

The proposals must cover the following activities as referred in Article 10(3) of the EDF Regulation, not excluding downstream eligible research activities if deemed useful to reach the objectives:

- activities aiming to create, underpin and improve knowledge, products and technologies, including disruptive technologies, which can achieve significant effects in the area of defence;
- activities aiming to increase interoperability and resilience, including secured production and exchange of data, to master critical defence technologies, to strengthen the security of supply or to enable the effective exploitation of results for defence products and technologies;
- studies, such as feasibility studies to explore the feasibility of new or improved technologies, products, processes, services and solutions.
- the design of a defence product, tangible or intangible component or technology as well as the definition of the technical specifications on which such design has been developed which may include partial tests for risk reduction in an industrial or representative environment.

Activity 1. Generating knowledge - Compiling background information

- Task 1: collecting data on parameters, characteristics, functioning and efficiency of currently used protection systems of heavy-armoured vehicles and infrastructure facilities (passive, reactive and active protection systems and their combinations);
- Task 2: identifying of weak points of currently used protection systems of heavy-armoured vehicles and infrastructure facilities (passive, reactive and active protection systems and their combinations);
- Task 3: defining potential strategies and methods of defeating protection systems of heavy-armoured vehicles and infrastructure facilities (passive, reactive and active protection systems and their combinations), that will take into account indicated weak points of their design and definition of the basic parameters of the developed combat system: type of the warhead used; number and type of shaped charges/EFP's/other charges (single, tandem, triple); type of the warhead carrier (grenade, mine, drone, *etc*.);
- Task 4: determining methods of increasing of the warheads effectiveness and defining design assumptions that will allow to implement the strategies of defeating protection systems for heavy-armoured vehicles and infrastructure objects defined in the previous tasks (passive, reactive and active protection systems and their combination);
- Task 5: identify state-of-the-art charge designs and manufacturing technologies of sub-components such as high explosive charges, shape charge liners, initiation systems and warhead casings.

Activity 2. Integrating knowledge - Initial warhead designs

- Task 1: evaluating numerical tools and developing numerical models of the warhead/target systems and performing computer simulations in order to initially evaluate the penetration capability of newly developed warheads;
- Task 2: warhead design developments integrating previously studied sub-component;
- Task 3: preparing warheads for experimental tests;
- Task 4: performing of experimental tests determining the functioning and the penetration capability of developed warheads.

Activity 3. Studies - Warhead optimization and munition applications

- Task 1: gathering and analysis of the results of experimental tests and numerical simulations determining the functioning and the penetration capability of developed warheads;
- Task 2: defining the directions of modification and optimization of the developed warheads in order to increase their penetration capability and the effectiveness of defeating protection systems of heavy-armoured vehicles and infrastructure objects (passive, reactive and active protection systems and their combinations);
- Task 3: developing initial concepts of new warhead carriers as well as selecting existing ones (grenades, mines, drones, *etc*.).

Activity 4. Design - Weapon system integration and validation

- Task 1: developing initial concepts of combat systems designs containing developed subsystems: warhead-carrier;
- Task 2: preparing combat systems variants for experimental pre-tests;
- Task 3: performing experimental pre-tests determining the functioning of the developed combat systems;
- Task 4: performing experimental pre-tests imitating the interaction of the developed combat systems with the protection systems of heavy-armoured vehicles and infrastructure facilities (passive, reactive and active protection systems and their combinations).

Functional requirements

Regardless of the chosen strategy of defeating targets equipped with ERA and APS, as well as the type of the warhead carrier, the confirmation of the proper functioning of the developed combat system will be based on the presence of the main armour perforation in the target equipped with ERA and APS. However, defining the precise requirements for the proper functioning of the developed combat system requires knowledge about the structure of the armour system that will be attacked. Collecting this knowledge and, consequently, specifying the requirements for the designed system will be the subject of the actions in this stage of the project.

It should be noted, however, that the functioning of the system, subsystems (warheads, warhead carriers) and individual warhead components should be checked at individual stages of the research. The effectiveness of the newly developed warheads and their components should be compared to the existing solutions. Analysis of the system operation should include:

- at system level, beside determining the presence/ absence of perforation of the main armour of the target, the analysis should include the detectability of the combat system as well as fake warheads/fake carriers by APS radars;
- at the level of the warhead subsystem, their effectiveness should be determined on the basis of the penetration depth of RHA steel plates placed behind the reactive armour cassettes, also as a function of standoff distance;
- at the level of the warhead carrier subsystem, depending on the adopted strategy of defeating target, the analysis should include, among others, the degree of synchronization (of warheads in the case of a tandem grenade; a programmed swarm in the case of using drones as carriers), the degree of detection of the carrier by APS, *etc*.;
- properties of the explosives should be analysed in terms of detonation parameters (velocity of detonation wave propagation, detonation pressure, detonation energy), structure homogeneity (uniform density distribution throughout the charge volume), geometric accuracy, *etc*.;

- analysis of the liners should include the homogeneity of their structure, shape and integrity of the jet/EFP during the formation process, the penetration capability of the jet/EFP as a function of standoff distance, *etc*.;
- in case of the shells of the warheads, their strength, accuracy and assembly repeatability should be analysed, allowing to obtain high parameters of jet/EFP while minimizing the weight of the shell.

The activities should include the development of new concepts and demonstrators for technologies like Explosively Formed Projectiles, Multi-Liner Explosively Formed Projectiles or Slow Stretching Shaped Charges. Furthermore, research could be conducted on an enhanced performance of shaped charges by applying new high explosives, new liner materials and geometries.

The activities should include the development of new concepts and demonstrators for geometries, materials, and fusing systems on small calibre penetrator warheads, which can be integrated in weapon systems used by ground forces.

The activities should also include pre-test campaigns with static and dynamic trials against both APS and ERA as well as infrastructure.

The desired technology readiness level (TRL) range is 4-5.

Expected impact

- The outcomes of the aforementioned activities enable EU Member States to engage effectively next generation main battle tanks.
- Recent conflicts have shown that without tandem warhead technologies, land forces would have been ineffective against adversary fighting vehicles with ERA. Since ERA is constantly further developed, both systems have to be addressed. The above mentioned approaches will provide an answer to both APS and ERAs.
- Moreover, EU members will be able to endow their ground forces with the capability to engage effectively infrastructure in the future.
- As multiple recent conflicts have shown, warfare will increasingly take place in urban terrain. Respective weapon systems used in this context have to deliver specific effects and reduce collateral damage.
- These outcomes will strengthen the EU's technological and industrial base and help warhead systems to overcome modern defensive technologies and to penetrate infrastructure with small calibre warheads. Already the availability of such technologies will deter aggressors and thereby contribute to Europe's security.

2.16. Call EDF-2021-GROUND-D: Fleet upgrade and close combat

Proposals are invited against any of the following topics:

- **EDF-2021-GROUND-D-FMGV:** Future modular ground vehicles and enabling technologies, including green technologies;

- **EDF-2021-GROUND-D-UGVT:** Unmanned ground vehicle technologies;
- **EDF-2021-GROUND-D-3CA**: BLOS collaborative close combat architecture.

Budget

The Union is considering a contribution of up to EUR 41 000 000 to support proposals addressing any of the abovementioned topics and their associated specific challenge, scope, targeted activities and functional requirements.

The budget earmarked on 2021 appropriations for this call will be completed by an amount of EUR 109 000 000 from 2022 appropriations. This complement is subject to the adoption of a separate financing decision.

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

2.16.1. Topic EDF-2021-GROUND-D-FMGV: Future modular ground vehicles and enabling technologies, including green technologies

The evolving operational environment requires the development of next generation and the modernisation of current armoured platforms with improved robustness, agility, versatility and interoperability. Moreover, future land vehicles will require the ability to operate in adverse conditions, in digitised battlefield and network centric environments, and to obtain scalable effects, while ensuring efficient maintainability and support, high level of operational readiness and optimized life cycle cost. This topic addresses mainly technologies enhancing the mobility performance of ground platforms, making them more capable, modular and energy-efficient.

Specific challenge

Future capability and operational challenges require the development of next generation and the modernisation of current platforms, armoured with enhanced interoperability, agility, survivability, mobility, durability, versatility, security including cyber, as well as the ability to operate in adverse conditions (facing challenging threats in various environments), addressing a large range of missions, in digitised battlefield and network centric environments, and to obtain scalable effects and other ground platforms such as logistic support vehicles, engineering vehicle, while ensuring efficient maintainability and support, high level of operational readiness and optimized life cycle cost. This topic addresses different technologies enhancing ground platforms' mobility performance and core operational functions and other enabling capabilities, which will make them more capable and energy-efficient to achieve these goals.

Due to existence of a number of different armoured land platforms, the complexity of joint and logistic capabilities is increased, and the effectiveness of public investment is decreased. The lack of European system of systems approach for the development of land platform capabilities has affected and inhibited the use of potential joint capabilities. Numerous existing armoured vehicles are aging and therefore do not meet users' capability needs anymore.

Land systems vehicle upgrade programs are a cost effective and fast way of extending the in-service life of existing military vehicle fleets. Opportunities exist to simultaneously extend the in-service life of a vehicle fleet and improve vehicle performance by effective design at any stage of the vehicle life cycle. Due to new challenges in military operations the land systems, in order to maintain their combat effectiveness, require upgrade processes to enhance both in protection (ballistic armour and protection systems) as well as mission kits, which typically increase the weight of the vehicles. Future programs provide opportunities to extend combat capabilities, to create game changers with respect to past and existing situations and to strengthen interoperability, maximizing impacts on cost-effectiveness and scale-effects. In particular, future vehicles should further protect troops through improved force protection, and stealth, extended situation awareness capability and autonomous functionalities, enhanced engagement capabilities, reduction of harmful vibrations, improved vehicle mobility through suspension upgrades, new technology for flexible tracks (elastomers) and implementation of electric/hydrogen/hybrid power packs and drivetrains.

Scope

Proposals must address the development of next generation or upgrade of current armoured platforms, in particular addressing Armoured Personnel Carrier (APC) and Light Armoured Vehicle (LAV) or developing and integrating modern and upgraded systems, subsystems like hybrid drivetrains and energy storage systems or sensors and a flexible network infrastructure into existing platforms and/or payloads improving significantly their performance. The proposals will thus possibly address other existing or future vehicles of various types and sizes such as Main Battle Tanks (MBT), Infantry Fighting Vehicles (IFV), support vehicles or Combat Engineering Vehicles (CEV).

Targeted activities

The proposals must cover the following activities as referred in Article 10(3) of the EDF Regulation, not excluding upstream or downstream activities eligible for development actions if deemed useful to reach the objectives:

- the design of a defence product, tangible or intangible component or technology as well as the definition of the technical specifications on which such design has been developed which may include partial tests for risk reduction in an industrial or representative environment;
- the development of a model of a defence product, tangible or intangible component or technology, which can demonstrate the element's performance in an operational environment (system prototype);
- the testing of product, tangible or intangible component or technology.

Functional requirements

Systems engineering activities should follow ISO/IEC 15288(2015) processes.

1. Mobility

Platforms' mobility must provide a substantial improvement of mobility compared to current platforms including, when appropriate, in an extreme environment (sand, ice, heat, cold), making them more capable and energy-efficient using green technologies and reducing the logistic footprint. Same platform should have high-level tactical and operational mobility. System should also have the capability of crossing water obstacles.

2. Enabling Capabilities

Modularity and commonality

Solutions of capabilities should be based on interoperability, modularity and commonality, which decrease complexity of joint and logistic capabilities of the platforms. They should maximize standardization, offering growth potential and further incremental improvements possibilities, based on a system-of-systems approach including open architecture concepts (*e.g.* NATO Generic Vehicle Architecture NGVA). This includes the potential integration and interoperability of manned and unmanned aerial and ground vehicles (UAV/UGV).

Drivetrains and energy systems

New platforms will have to export sufficient electric energy for mission and role kits. Here is the need for electrical energy storage, supply and management systems, new running gear and possible new drivetrain systems *e.g.* hybrid to provide high levels of energy production under degraded condition. This combination should improve the operational life and the efficiency of engines and power packs.

Survivability

Platform protection should be modular by design and according to the threat and/or the specific mission. Platform must be capable of performing their missions under chemical, biological, radiological and nuclear (CBRN) conditions and counter a variety of threats such as kinetic, IED/EFP, UAV ones. Platform should have low visual, thermal, electromagnetic, noise and radar signatures. Platform must be capable of performing their missions, by day, night in extreme environmental conditions. Platforms should be cyber resilient and provide cybersecurity, given the increasing connectivity of systems expected.

Command and control

System should enable high interoperability, through use of common standards and open architectures. Systems should be prepared for optionally manned/unmanned operations. System should be able to accommodate applicable military radio transmitters and receivers during operation and when at a silent watch (not to exclude the use of any military radios due to bad electromagnetic compatibility (EMC)). Platform should integrate Battle Management Systems (BMS), SATCOM, target hand over and have an advanced Position Navigation and Timing system in contested and denied environment. The system should address the vehicles internal network and the network capabilities between vehicles. The requirements for network support for collaboration with dismounted personnel or remotely controlled/robotic elements should be covered.

Situational Awareness

Implementing emerging technologies/systems should substantially increase situational awareness of platforms compared to current versions, allowing a 360º situational awareness, automatic threat detection, tracking and identification, real time updated and shared operational picture and information. Technologies should enhance the survivability by offering to the crew situation awareness information. Implementing technologies/systems should minimize detection and response time toward entities/potential threats and/or enhance main weapons' effectors (*e.g.* through the use of sensors). Situational awareness system architecture should be open to facilitate integration to any armoured vehicle.

Engagement

System should enable payloads capability. The system should be optimized to carry out different role tasks according to their specific performance criteria (*e.g.* troop carrier or fire support or recce). For the lighter vehicles weapon systems should be removable. Remote weapon station should be considered for small and even medium calibre.

Life Cycle Support

Next generation platforms must feature such a maintainability in solution design in order to enable greater operational availability/readiness at lower total cost of ownership compared to current platform. Platforms' or systems' acquisition cost should be lower than current platforms. The target for platforms' efficient operational lifecycle should be at least 30 years.

Growth Potential

The development of modular systems and a marked open architecture will ensure agile and continuous growth, especially of higher-tech components (C2/C5ISTAR, lethality systems). System designs will include suitable availability of payload, volume and energy production in order to enable the continuous upgrade of the overall platform's performances and functions.

Expected impact

The proposed solution should:

- increase EU industrial capability to produce advanced concepts and new highly innovative vehicle systems with a view to extend combat capabilities and to create game changers with respect to past and existing situations;
- provide solutions that solve future capability needs of Member States with maximum commonality and modularity;
- provide a technological building blocks useful for future vehicles or for extending the in-service life of existing military vehicle fleets;
- provide vehicle solutions, which have a reduced environmental and logistic footprint;
- provide opportunities to eliminate or limit environmentally toxic substances;
- establish European business consortia able to offer competitive solutions for global markets, maximizing impacts on cost-effectiveness and scale-effects, while stimulating industrial cross border cooperation;

- reduce strongly the dependence from non-EU technologies and products and by that increase the EU's Security of Supply of armoured vehicles and related systems.

2.16.2. Topic EDF-2021-GROUND-D-UGVT: Unmanned ground vehicle technologies

There are significant cooperation opportunities in the Union regarding unmanned systems, which could be based on a shared operational concept and the resulting harmonisation of requirements. Moreover, the CDP analysis identifies the need to deploy unmanned systems to reduce the danger to human personnel and manned platforms, as well as to increase robustness, sustainability and resilience of ground systems. A comprehensive set of unmanned systems should contribute to the capability of land manoeuvre in the joint operational environment to gain positional advantage in respect to the adversary. Purely unmanned tracked vehicles as funded under EDIDP will not be considered under this topic.

Specific challenge

Most military experts and strategists agree that the ability to conduct swarm operations is probably the best response to future threats whether symmetrical or asymmetrical. In this context, it is therefore vital to have the ability to design and conduct long-distance operations against a highly mobile and unpredictable enemy through the flexible use of a significant number of unmanned and coordinated ground and air systems.

Indeed, intelligent and effective cooperation between unmanned ground systems (UGS), manned military vehicles, operators and air systems is needed to increase the robustness, sustainability and resilience of these terrestrial systems while reducing loss of life, the risk of collateral damage and lowering the cognitive burden placed upon operators.

Deploying a swarm-based manoeuvring capability in a framework of cooperation between manned and unmanned systems (manned-unmanned teaming) but also inside the swarm of unmanned systems is undoubtedly the strongest requirement in system design in the field of safety research.

Therefore, rapidly developing a capacity implies an incremental approach capable of proposing capability milestones in line with the development milestones of current and future land systems and allowing upgrades of legacy systems.

Scope

Proposals should address the development of hardware or software modules designed to enable manned-unmanned operation modes and taking into account teaming and swarming, and to be integrated or embedded into a set of digitalised ground Armoured Vehicles (fielded, still under development or future) and showing the following capabilities:

- to interconnect in real time and in a fully secured way an extended set of systems supported by an intelligent management solution and by operational aid modules;
- to be integrated in a manned digitised vehicle to make it temporary unmanned for specific parts of the mission;
- to propose real-time "reflex actions" to increase force protection and impacts of actions;

- to cooperate with the rest of the combined armed company while being able to enter, remain and exit the company network and to interact with unmanned ground vehicles (UGV) and unmanned aerial vehicles (UAV);
- to enable a versatile use in order to be deployed for a large spectrum of operational missions and provide operation capability in hostile, harsh environment;
- to be compliant with ethics and regulations regardless of the operational context.

Targeted activities

The proposals must cover the following activities as referred in Article 10(3) of the EDF Regulation, not excluding downstream activities eligible for development actions if deemed useful to reach the objectives:

- studies, such as feasibility studies to explore the feasibility of new or improved technologies, products, processes, services and solutions;
- the design of a defence product, tangible or intangible component or technology as well as the definition of the technical specifications on which such design has been developed which may include partial tests for risk reduction in an industrial or representative environment;
- the development of a model of a defence product, tangible or intangible component or technology, which can demonstrate the element's performance in an operational environment (system prototype).

The proposals must address in particular the following objectives:

Studies

- autonomous behaviour understanding (Risks, ethics, Rules of engagement, decision making support);
- definition of targeted vehicles (fielded or under development or future);
- analysis of civilian/military communication and data exchange standards of the targeted vehicles;
- analysis of commonality of requirements and functionalities for the targeted vehicles;
- definition of CONOPS (Concept of Operations) related to the relevant functions for the targeted vehicles;

Design

- definition of the relevant functions related to relevant manned-unmanned operation modes for teaming and swarming, environment understanding and advanced decision-making support;
- definition of their implementation and integration into the system architecture of the targeted vehicles (hardware, software, networks);

- definition of the security environment; development of solutions for manned to unmanned transformation, teaming, swarming, environment understanding and advanced decision-making support;
- definition of open solutions able to embed future sensors and sensor systems;
- proposal for a test case as a basis for demonstration, simulation and prototyping;

Prototyping for implementation of selected use cases (to be consolidated along the project implementation)

- integration of a system demonstrator for:
  - risk mitigation;
  - presentation of study results and execution of a demonstration with a test scenario.

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.

Functional requirements

Development of functions that enables upgrading a set of current vehicles or to be integrated into vehicles under development or future vehicles with the ability to embed advanced multi-technology sensors networks and advanced effectors networks around a common and standardised manned/unmanned teaming capability.

This set of modular components will provide Armoured Fighting Vehicles programs with the capacities to operate within connected hybrid manned/unmanned teams with the following main functional requirements around a common and standardized manned-unmanned teaming core function:

- ability to timely and swiftly shift a vehicle in an unmanned configuration;
- ability to manoeuvre the unmanned vehicles as needed for the relevant functions both in autonomous and remote way since:
  - an unmanned vehicle can be remotely driven from any position (manned vehicles, possibly moving, operational station, *etc*.);
  - the operators must have a comprehensive understanding of the environment of remote unmanned vehicles;
  - the operators must rely on operation aids, autonomous functionalities with a special care in the reduction of collateral damage risks**;**
- ability to interact and manoeuvre within a manned-unmanned swarm and possibly to resort to advanced interaction modes;

- ability to understand the operational and tactical environment to speed up the decision-making process of the operators by delivering a user-friendly and reliable decision-making support tool that enables them (him/her) to remotely operate all the payload from any of the manned vehicles by:
  - providing real-time trustable situational information and information sharing inside the swarm;
  - allowing to remotely operate the effectors the relevant vehicles (manned and unmanned) in order to gain a tactical advantage and generate tactical options, taking into account the tactical required effects, the collateral damage constraints and the ethical aspects;
- ability to seamlessly and securely add external UGV or UAV in order to enhance drastically capabilities in the following domains:
  - force protection against a large spectrum of threats by using UGV especially dedicated to a specific domain;
  - integration of Beyond Line Of Sight (BLOS) detection capabilities;
- ability to increase force protection and resilience through:
  - indistinguishability between manned and unmanned platforms:
    - to prevent external identification of an uninhabited or inhabited vehicle to target it as a priority (doesn't apply to vehicles designed to be only used in unmanned mode);
    - to give access to this capacity without increasing the logistic footprint;
  - the improvement of sensors' efficiency and real-time communication;
- the diversity of sensors to ensure the availability of information;
- state-of-the-art system with modern, customizable and intuitive user interfaces that support operators in all their operational, technical and training needs. Deployability must be the cornerstone of system design, enabling rapid adaptation, implementation, operation and training;
- ability to operate in all relevant European climate zones or in all area where relevant EU missions could be conducted;
- the functions must be dynamic, scalable and resilient, efficiently embeddable in most of existing ground combat vehicles systems, compliant with their different programme roadmaps and their modules' obsolescence lifecycles;
- the functions as designed must be able to support specified availability requirements to contribute to an open, scalable, highly available and transparent failover architecture;
- the functions as designed must be proof against diminution of environmental sensing capability, hostile countermeasures, including the application opportunity in Global Navigation Satellite System (GNSS) denied operation environment;

- 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;
- the functions as designed must be able to work simultaneously in different security environments and handle the information security requirements to properly control the information flows between these domains and with external systems. The system must be able to be integrated into environments that impose different security constraints on the exchange of information while remaining usable in an environment with low security constraints;
- the function must be designed in accordance with the modularity principle in order to enable integration of new technological solutions and to enable obsolescence management;
- a human operator must remain in the loop prior to the employment of any effectors while passive sensors can potentially be employed autonomously to increase the potential capacity to gather data and increase situational awareness;
- the functions as designed must comply or be able to comply with the operational procedures of the targeted vehicles, with ethical and environmental constraints as well as with logistic and defence program efficiency requirements.

Expected impact

- Develop critical enablers for Common Security and Defence Policy (CSDP) operations and EU Battlegroup missions.
- Enhance force protection.
- Reduce the minimum reaction time for deployment of EU military missions.
- Reduce the possible number of casualties on friendly forces.
- Interoperability milestones for Member States' ground capacity programs.
- Improve situational awareness, resilience and security of EU operations.
- Create a reference for manned-unmanned teaming modes and functions that will improve the capabilities of the European defence industry to develop and supply state-of-the-art ground systems.
- Reinforce interoperability of EU Member States' armed forces.
- Strengthen the EU's strategic autonomy in military capabilities.
- Increase interoperability and synchronization between manned and unmanned platforms, and soldier systems.
- Reduce the cost of European military missions.
- Reduce the impact of the logistic footprint.

2.16.3. Topic EDF-2021-GROUND-D-3CA: BLOS collaborative close combat architecture

The availability of mobile precision systems able to provide the necessary high degree of accuracy and efficiency, avoiding widespread collateral damage, and reducing exposure of friendly forces is a priority for Member States' armed forces. In this context, some requirements are becoming increasingly important, *e.g.* to provide the land and naval combat units with the ability to defeat at medium and long ranges, and with a very high degree of accuracy and reliability. In order to meet these requirements, research activities on a Beyond Line Of Sight (BLOS) collaborative close combat architecture are required.

Specific challenge

The EU is facing increased geostrategic instability. Land and naval combat units of EU Member States have to address on the battlefield a complex set of conventional and new threats. They have to intervene in a high intensity and in asymmetric engagement, facing a wide range of threats including potential technically advanced adversaries.

To succeed in BLOS-firing mission, reconnaissance, intelligence and adequate preparations will be essential. A technical system design (incorporating C2, mobility, survivability, lethality, intelligence and endurance) for BLOS will need to be versatile against future alterations pending an evolving hostile threat. A BLOS system design will need to be robust and secured against the future to motivate investments in resources and funds for the anticipated period of life.

In this context some requirements are becoming increasingly important: provide the land and naval combat units with the ability to defeat at medium and long ranges, with a very high degree of accuracy and reliability, selected threats that are not always clearly identified and visible or defeat targets that may mask or unmask at the last moment; reduce exposure to enemy fire; avoid widespread collateral damage; allow concentrating fires without concentrating means, providing autonomy, reactivity and freedom of action at the level of the combat units on the battlefield.

Scope

Development of a BLOS collaborative close combat architecture based on BLOS native missile systems (with full Lock-On After Launch (LOAL) and Man-In-The-Loop (MITL) capabilities through a seeker back-image):

- multi-domains (land/air/sea);
- multi-platforms integration (air/land/naval, manned/unmanned);
- multi-sensors (alert, detection, target designation, engagement);
- explore and define system architecture;
- study and develop an enhanced BLOS concept according to defined system architecture;
- define, study and develop interfaces for supporting systems, hardware and applications serving to enhance BLOS-capability;

- extended range;
- cooperative engagement;
- enhanced performances and functional capability;
- increased robustness to aggressions (cyber, jamming);
- innovative technologies insertion;
- mission planning and decision-making supported by AI;
- design and develop concept for training and evaluation of BLOS capability involving interoperability among Member States.

Targeted activities

The proposals must cover the following activities as referred in Article 10(3) of the EDF Regulation, not excluding upstream or downstream activities eligible for development actions if deemed useful to reach the objectives:

- studies, such as feasibility studies to explore the feasibility of new or improved technologies, products, processes, services and solutions;
- the design of a defence product, tangible or intangible component or technology as well as the definition of the technical specifications on which such design has been developed which may include partial tests for risk reduction in an industrial or representative environment;
- the development of a model of a defence product, tangible or intangible component or technology, which can demonstrate the element's performance in an operational environment (system prototype);
- the testing of product, tangible or intangible component or technology.

Functional requirements

The BLOS Effect – Collaborative Close Combat Architecture must provide the following Capabilities:

A1. The system must have the capacity to be operable day and night;

A2. The system must be compatible with climates met in Europe as well as in Africa and other continents, in winter and summer conditions;

A3. The missile must have the possibility to engage targets at 400 m in LOS Fire and Forget mode;

A4. The missile should have the possibility to engage targets at 200 m in LOS Fire and Forget mode;

A5. The BLOS system must have an effective range of at least 4000 m;

A6. The system must be a close combat capacity with minimal reaction time (platoon coordination);

A7. The BLOS system must be both man-portable as well as integrated on vehicle platforms;

A8. The BLOS system must have a capability to engage targets in a direct fire mode. The system must also be able to engage targets in an indirect fire mode using target coordinates and/or associated image;

A9. The BLOS missiles must have a back-image capability (image sent from the missile to the user) for target acquisition and lock on during flight on operator action in the platform;

A10. The BLOS system must have the possibility to stream the real-live images (the back image of the missile flight as well as of the drone) as well as to record it on a specific man-portable and ruggedized connected device that is standard equipment of the BLOS Firing Team;

A11. The ruggedized connection device must allow the simultaneous livestream of both missile image and drone feed. The image screen and resolution must be good enough to allow a qualitative display of the backward images;

A12. The BLOS system must be transportable by road (logistic, tactical transport and on launch pod), sea and air;

A13. The negative influence of the transport on the lifespan of the system must be less than or equal to existing comparable systems;

A14. The BLOS systems levels of safety, functionality and reliability must not be decreased from logistical and tactical transport corresponding to the Member State’s needs;

A15. The UAV must have the capability to designate a target, in terms of coordinates in the referential common to the platform with the required accuracy (sensor and software payload adaptation on micro drone to reach the required accuracy);

A16. The UAV must be able to navigate and designate targets in a GPS-denied environment;

A17. The time to transport the UAV, to deploy and to operate must be minimized by the design;

A18. UAV must be used and recovered from a moving or a fix vehicle;

A19. Operational range of the UAV must be beyond 4000 m from its remote pilot, taking into account that the targets are partly dissimulated and only visible from 3500 m;

A20. The UAV must be operable without line of sight between the remote pilot and the UAV to assist BLOS missions;

A21. The speed of the UAV must be compatible with the CONOPS of the Member States;

A22. The data links must be cyber robust (to its control base), the cyber aspects being fully controlled by Member States;

A23. The technologies and components of the system must be built with a European design authority, must not contain any IPR generated outside Europe and must be free of any third-party control regime.

The initial BLOS capability must be enhanced:

B1. The BLOS system must be man portable, able to operate on ground, as well as mounted on various platforms such as vehicle, naval platform and UGV;

B2. The BLOS system must re-inforce its protection capability such as peripheral observation, target designation and response to threats directed at the BLOS-system itself;

B3. The BLOS system must be able to receive targets cueing from several sub-systems (recce team, UAV, UGV, *etc*.);

B4. Manoeuvre and engagement of the BLOS system must be prepared, the BLOS system must integrate a system to manage immediate mission planning and engagement; the mission planning system must be fully interoperable with the battlefield management systems of participants;

B5. The BLOS system must have an associated battlefield training system for indoor and outdoor exercises;

B6. The BLOS battlefield training system must support realistic live training force on force (f2f) for all user scenarios, incorporating collaborative uses of target designation (recce team, UAV, UGV, *etc.*);

B7. The BLOS battlefield training system must include an outdoor training system capable of training the full BLOS capability;

B8. The BLOS Battlefield outdoor training system must have the possibility to make use of enhanced reality targets;

B9. The BLOS Battlefield outdoor training system must as much as possible make use of the BLOS Combat Systems components;

B10. The BLOS battlefield trainer must have a terrain representation enabling it to pre-evaluate a fire mission. The BLOS training system must propose a tool to support evaluation of tactics for the system;

B11. The study must explore the possibility of a common architecture for the BLOS training system (indoor, outdoor and pre-mission);

B12. The BLOS battlefield trainer must have a terrain representation enabling it to pre-evaluate a fire mission, including good level of representation of trajectory and sensors parameters;

B13. The BLOS training systems must be connected to exercise control structure (EXCON) for monitoring players during f2f live training;

B14. The study must explore the possibility to display a realistic signature effect (flash and bang effect) in the BLOS training system;

B15. The BLOS system must be coordinated at platoon and squadron/company level, it must operate with cooperation means such as communication network or participants or European Battle Management System;

B16. Interoperability of the BLOS system with a set of existing weapon stations must be studied;

B17. UAV system must have the ability of integration into collaborative combat threw BMS interoperability;

B18. The study must explore the possibility to include a device that informs that the aerial is entering an opponent's jamming zone.

The initial BLOS capability must be extended to BLOS Extended Range (BLOS ER) and BLOS Next Generation (BLOS NG) capabilities:

C1. Compatibility of the BLOS ER and BLOS NG systems with the BLOS launching station (man portable as well as platform integrated) must be studied;

C2. The BLOS ER system must operate with an operational range up to 8 km and detection, recognition and identification capability up to 10 km;

C3. The BLOS ER missile must have a hand-over functional capability from SAL to back image;

C4. The BLOS ER system must operate with different platforms such as helicopter, naval, UAV (*e.g.* MALE), on the ground and mounted on ground vehicle;

C5. The BLOS ER and BLOS NG systems must improve the over-all engagement functions and associated sub-systems (optical and inertial sensors, UAV…);

C6. The BLOS NG architecture must integrate new technologies such as ATR (Automatic Target Recognition), potentially using Artificial Intelligence (AI), sensors data fusion and robust navigation functions;

C7. The BLOS NG system will be compatible with the initial BLOS system.

Expected impact

- Contribute to the defence and security interests of the EU and its Member States.
- Contribute to the EU strategic autonomy level of ambition.
- Address the EU ground combat capability development priority identified as part of the revised 2018 CDP and contribute to the objective of the PESCO BLOS capability project which is to develop under a European design authority a new generation of BLOS missile systems family.
- Bring a significant operational differentiator to the land and naval combat units of the Member States by providing an engagement capability with a very high degree of accuracy while avoiding widespread collateral damage, and reducing exposure of friendly forces.
- Contribute to enhanced interoperability between armed forces of the Member States, stimulate European doctrine and European standards.
- Contribute to Europe’s resilience and European technological sovereignty.
- Contribution to European industrial autonomy.

- Contribution to excellence with the demonstration of a significant advantage over existing products or technologies.
- Contribution to innovation through the application of technologies and concepts previously not applied in the defence sector.
- Contribution to strengthening the competitiveness of the EDTIB by creating new market opportunities.
- Contribution to relocate some technologies and expertise in Europe and under a European design authority in line with the EU industrial autonomy and technological sovereignty ambitions.

2.17. Call EDF-2021-PROTMOB-D: Soldier & logistic systems

Proposals are invited against any of the following topics:

- **EDF-2021-PROTMOB-D-SS:** Development of full-size demonstrators for soldier systems;
- **EDF-2021-PROTMOB-D-DMM:** Development of a digital system for the secure and quick exchange of information related to military mobility.

Budget

The Union is considering a contribution of up to EUR 50 000 000 to support proposals addressing any of the abovementioned topics and their associated specific challenge, scope, targeted activities and functional requirements.

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

2.17.1. Topic EDF-2021-PROTMOB-D-SS: Development of full-size demonstrators for soldier systems

Soldier Systems support force protection, increase operational effectiveness, reliability and endurance of individual soldiers and formations. They comprise the gender-neutral equipment of individual military personnel to be able to operate with a sufficient level of protection in any operational environment. Soldier Systems are a primary force multiplier. The development and integration of cutting-edge technology is key for forces.

Specific challenge

The evolving operational environment requires the development of a next generation dismounted soldier system able to enhance close combat operational capabilities such as survivability facing new threats in various operational theatres, mobility, lethality, command and control and sustainability, as well as training and simulation embedded systems to enhance readiness. It should be designed for an easy integration in a digital battlefield thanks to interoperability features with next and upgraded armoured land and airborne vehicles as well as future unmanned vehicles (UxVs) along with already deployed upgraded soldier systems.

This new generation system focuses on empowering soldier tactical decision ability that becomes more efficient within his tactical organization through a common pool of resources.

Individual capability enhancement and a comprehensive integration of soldiers in the digital battlefield should contribute to the dominance in joint operational environments for the troops in that operational environment.

Specific challenge of individual capability enhancement address the dismounted close combat domains (C4I, survivability including protections, mobility, lethality, sustainability) focusing on the reduction of the burden of the soldier while optimizing the cognitive load under operational conditions.

Scope

The proposals must address:

- the development of an individual advanced standardized and open architecture soldier core system able to integrate devices, capability suites and applications meeting this standard able to guarantee an agile process for a rapid evolution of the dismounted soldier's operational capability facing an evolving operational environment;
- innovative technologies for new devices and capability suites development able to be implemented / integrated with the soldier core system addressing the domains of the close combat, *i.e.*: survivability (multi-threats protection, threat detection), sustainability (enhancement of energy source capacity and power management), mobility (localization, navigation and physical augmentation), observation (environment perception and situational awareness by day and night conditions), lethality (smart engagement), along with path-agnostic communications[75]. These innovative technologies will rely on advanced technologies such as data sciences;
- new networking capability developing mixed interactions between soldiers, armoured vehicles and UxVs in an augmented tactical unit format relying on standard interface and protocols consistent with existing or coming next tactical communication (*i.e.*: shared situational awareness and localization when dismounted and while dismounted from vehicles carriers, combat id, coordinated navigation, collaborative observation and protection, coordinated fire support with available weapon systems at tactical unit level);
- the above topics must show a clear vision for a harmonization process of requirements, specifications and standards able to demonstrate economical, technical and operational advantages to promote future European acquisition plans.

[75] Capability to communicate reliably to any location in the world without explicitly specifying which nodes of a communication network to use.

Targeted activities

The proposals must cover the following activities as referred in Article 10(3) of the EDF Regulation, not excluding upstream or downstream activities eligible for development actions if deemed useful to reach the objectives:

- studies, such as feasibility studies to explore the feasibility of new or improved technologies, products, processes, services and solutions;
- the design of a defence product, tangible or intangible component or technology as well as the definition of the technical specifications on which such design has been developed which may include partial tests for risk reduction in an industrial or representative environment;
- the development of a model of a defence product, tangible or intangible component or technology, which can demonstrate the element's performance in an operational environment (system prototype);
- the testing of product, tangible or intangible component or technology.

Functional requirements

The targeted activities must address:

- harmonization activities for requirements, specifications and standards through a large cross-fertilization process with Member States representatives in all domains (OPS, TECH, Procurement…). The harmonization approach assessment is done through:
  - definition of Use Cases and *ad-hoc* concepts of operations (CONOPS);
  - specification, design and development of an open soldier core system, which will consider the PADR GOSSRA (Generic Open Soldier System Reference Architecture) outputs executed under EDA STASS-II projects;
  - specification, design and development of capability suites interfaced with the soldier core system;
  - specification, design and development of network enable capability and new interactions with robotics and platforms;
- development of demonstrators/demonstration for evaluation purpose showing operational benefits and added value of harmonization activities with:
  - a feasibility study of the soldier system concept and a selection of devices/capability suites concepts connected to the soldier core system which fulfill the given high level requirements, including a Detailed Requirements Review (DRR);
  - the detailed design of the soldier system and selected devices / capability suites sub-systems, including a System Requirement Review (SRR), a Preliminary Design Review (PDR) and Critical Design Review (CDR);
  - the development, production and evaluation in a representative environment (virtual and/or real) of technology demonstrators (soldier systems – devices / capability suites)

able to be used in a representative scale demonstration making sense at the operational level and relying on tailored existing troop carriers armoured vehicles and UxVs;

- benchmarking/testing of the demonstrators against the requirements;

- synthesis and way to proceed for dissemination.

The soldier system and related devices/capability suites sub-systems must:

- have a system approach including standardization and open architecture concept to guarantee a rapid evolution of the system in a cost effective way;
- enhance operational capability in the supra mentioned dismounted close combat domains including logistic footprint and compatible with the system approach contributing to size, weight, power and cost (SWaP-C) criteria;
- demonstrate secured networking enable capabilities at the tactical unit organization level involving armoured troops carriers and UxVs.

To fulfill above mentioned requirements the soldier core system solution must:

- focus on lightweight, modularity, ergonomic and highly usable man/system interfaces;
- federate relevant upcoming technology building block (TBB) studies and existing/already performed TBBs study outcomes;
- consider experience learned from existing deployed soldier system.

To fulfil supra mentioned requirements the soldier system and the related devices / capability suites must:

- demonstrate substantial augmentation of dismounted close combat capability in the field of perception/situation awareness, mobility, localization/navigation and cognition thanks to multi modals interface concept and the support of Artificial Intelligence;
- be capable to interact with small new generation robotics and drones or upgraded ones;
- be compatible with military environmental conditions and capable of performing missions by day and night;
- be prepared to interface new dismounted weapon systems or upgraded ones to improve individual performance and enabling networking capability;
- support use of tactical communications;
- be prepared to interface the land tactical cloud;
- optimize the integration and connectivity with existing and coming next generation of troop carriers with respect to seamless communication and situational awareness in the mounted/dismounted combat phase;
- be designed to implement embedded training to facilitate system usability on the field;
- be design to interface training/simulation capability tools;
- minimize logistic footprint thanks to standardization;

- be capable to protect from CBRN threats;
- be designed to implement cybersecurity mechanisms protecting the integrity and security of the mission information;
- be prepared to assure the electromagnetic security (*e.g.* protection against jamming).

In the frame of the development process, the project should be scheduled according to:

- a two-year phase of requirements harmonization and enhancement of technologies readiness until getting a CDR gate;
- followed by a two-year development of demonstrators / demonstrations for operational evaluation purpose as well as the development of a dissemination process.

Expected impact

- Provide harmonized solutions for future capability needs of European Member States thanks to joint requirements, specifications and standards suitable for Armed Forces transformation process.
- Develop new innovative soldier technologies and capabilities in the domains of the dismounted close combat adopted by Member States Armed Forces.
- Enhance/reinforce EU industry capability to produce new highly innovative soldier systems, devices and capability suites for European soldiers.
- Establish a European business-oriented consortium able to offer European-based competitive solutions to address global market.
- Decrease dependence from non-EU technologies and products.

2.17.2. Topic EDF-2021-PROTMOB-D-DMM: Development of a digital system for the secure and quick exchange of information related to military mobility

Timely and accurate logistic information and sharing is required for the efficient management and coordination of multinational logistic networks and hubs. Information management for multinational logistics, including for Military Mobility related information, contributes to enhanced efficiency and effectiveness, notably to the reduction of overall costs and environmental footprint, flexibility of forces, improved interoperability and fair burden sharing between Member States or conservation of scarce local resources.

Specific challenge

The crises in the vicinity of the EU have changed the security situation of the EU Member States and EU needs to respond to those challenges. Inter alia, this significantly increases the importance of functioning and efficient military mobility. The ongoing COVID-19 crisis, although a civilian crisis, has painfully highlighted the gaps in the functioning of logistics in the midst of a crisis. In part, the problem is related to divergent requirements for the exchange of information on military mobility across the Member States. That has led to cumbersome and often slow cross-border movement.

The EU Foreign Affairs Council conclusions from 25 June 2018 put forward several political objectives concerning military mobility. Inter alia, they call on Member States to take action nationally to improve the efficiency of military mobility, and to simplify and standardise the relevant rules and procedures by no later than 2024. The Council conclusions further call for simplified and standardised procedures in order to accelerate border crossing procedures and work towards granting cross border movement permissions, including requests for entry and movement permission for all modes (surface, air and sea) for routine activities within 5 working days. Hence, this constitutes a strategic objective for the Member States.

A particular challenge is that, in practice, the time required to obtain approvals and diplomatic clearances for cross-border movements varies considerably between the EU Member States and the procedures are poorly standardised. Currently various approvals are needed at state, regional and local levels. Furthermore, there is a need to exchange customs related information digitally. As a result, the current situation has made the movement of troops, equipment and supplies slow and cumbersome.

Therefore, digital tools should be utilised to achieve the political objectives of greater simplification, standardisation and rapid issuance of the cross-border movement permits. To this end, a digital system for military mobility will be a key enabler for the political commitments made. Furthermore, military mobility is an area of flagship cooperation between the EU and NATO. The digitalisation efforts would support the work and objectives of both organisations. Therefore, the actions should be coordinated between the two organisations to the extent possible.

Scope

Digitalisation is a key enabler for efficient and speedy military mobility. Digitalisation would also allow for increased standardisation and harmonisation between the Member States. The scope of the action focuses on cross-border movement permissions. Currently, there are several different forms in use across the EU and NATO countries, whereas the authorisations that are needed differ at state, regional and local levels. Diverging rules, in turn, make the permitting procedures cumbersome and time-consuming. A joint ICT system should be used to develop uniform cross-border movement permission documents, which will be tailored to the needs of the participating Member States. Furthermore, there is ongoing work by the Member States and the EDA, which could be used as a point of departure.

The proposal must address the development of digital military mobility information exchange system.

Targeted activities

The proposals must cover the following activities as referred in Article 10(3) of the EDF Regulation, not excluding possible upstream and downstream activities eligible for development actions if deemed useful to reach the objectives:

- studies, such as feasibility studies to explore the feasibility of new or improved technologies, products, processes, services and solutions;

- the design of a defence product, tangible or intangible component or technology as well as the definition of the technical specifications on which such design has been developed which may include partial tests for risk reduction in an industrial or representative environment;
- the development of a model of a defence product, tangible or intangible component or technology, which can demonstrate the element's performance in an operational environment (system prototype);
- the testing of a defence product, tangible or intangible component or technology.

The proposals must address in particular the following objectives:

- **Objective 1**: feasibility study, identifying costs and benefits, assessment of the feasibility of possible functionalities and interfaces with the existing systems. Validation of the estimated budget (life cycle costs, including later maintenance costs) and assessment of the duration for the development. Final validation of the feasibility of the functional requirements;
- **Objective 2**: system Requirement Analysis detailing the needs based on the functional requirements, including analysis of end-user needs and the analysis of existing procedures;
- **Objective 3**: development and testing of a digital system for the secure and quick exchange of information related to military mobility. Development and testing to be done in close cooperation with the participating Member States and associated organisations. Training for the end-users and compiling user manuals.

Functional requirements

The Digital Military Mobility System for Cross Border Movement should be designed in line with the following principles:

(1) General:

- secure and fast cross border military movement digital information exchange between sending and receiving nations from the submission of the request to the final approval and response. The digital system must replace existing channels of communications like e-mail, fax, *etc*. with the purpose of consolidating and speeding up the flow of information and to prevent communications errors;
- one single system for different roles and counterparts related to cross border movement approval process. It may also include military movement management in case where the actual carrier is a private company.

(2) Security:

- encrypted web-based (online) system with a centralised server;
- UNCLASSIFIED level system with restricted access;
- secure authentication and authorisation of the systems users (two-step authentication);
- adequate cyber resilience of the system;

- data integrity and secure data exchange;
- user account management via national account manager (national single point of contact);
- access to information based on “need to know” principle. Member nation can only see the requests they have submitted or which are sent to them and they do not have access to the other nations´ information;
- cooperation (as appropriate) with eu-LISA and drawing on their expertise and know-how.

(3) Interoperability and interfaces:

- cooperation (as appropriate) with NATO and its member states in line with the EDF Regulation;
- interoperability and compatibility with, and allowing for automated (or partly automated) data (Excel/HTML transfer) exchange with:
  - NATO LOGFAS EVE (Logistics Functional Area Services, Effective Visible Execution);
  - EATC MEAT (Management of European Air Transport);
  - existing and/or under development HNS digital systems and national systems;
  - national movement systems;
  - national customs systems for customs Form 302 authorizations;
- interoperability with other digital systems as appropriate (for instance EU military customs system, if developed);
- to ensure better data exchange sharing and archiving processes for military products and systems it is envisioned that standards like ISO 10303 and ASD/AIS S-series standards could be beneficial to manage interoperability between user nations.

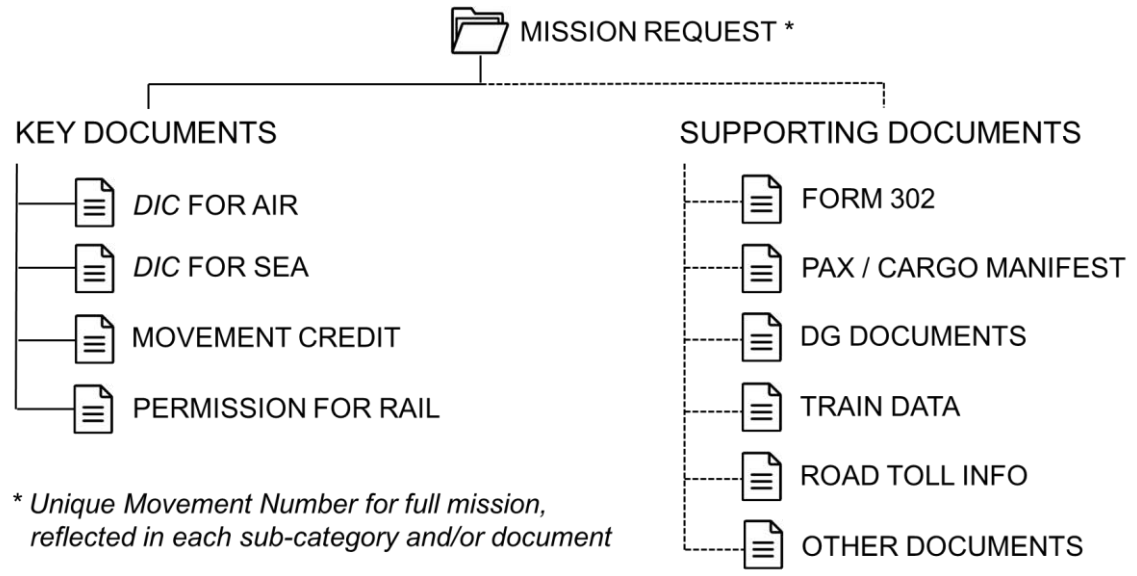
(4) Military Mobility related documents and information:

- standardised procedures and formats between sending and receiving nations, including harmonisation and simplification if possible;
- Web-based system that would allow the digital exchange of the following military movement information (see drawings in (5) and (6) below):
  - to notify, request and approve:
    - permit to deploy (request for visit);
    - diplomatic clearance for state aircraft;
    - diplomatic clearance for military vessel;
    - movement credit for convoy and oversize/overweight equipment;
    - rail permission;

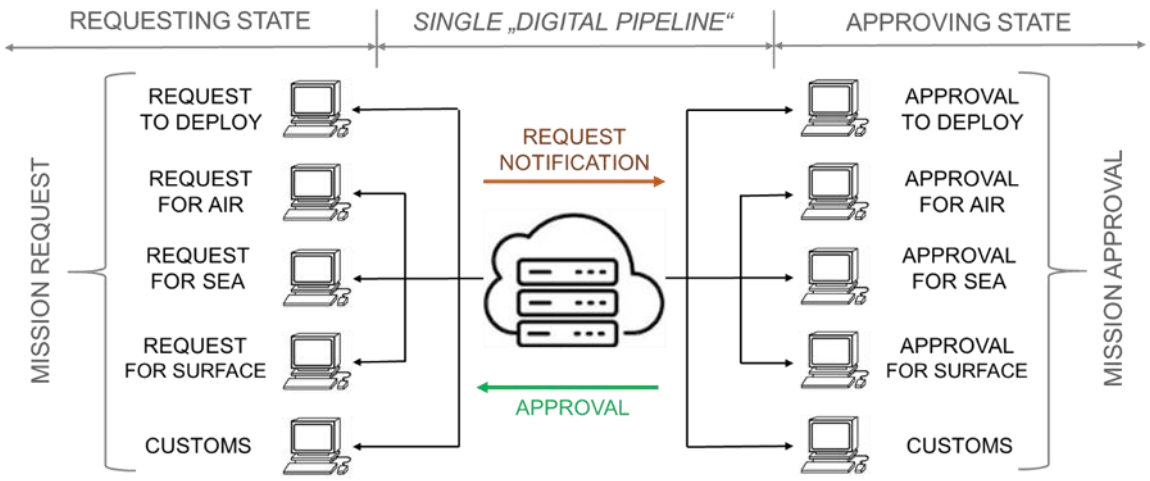
- to create and transfer customs documents (EU and NATO Form 302);
- to create or upload shipping documents (including dangerous good documents).
- to upload additional movement related documents and information according to the specific movement or operation;

- functionality for fast track approvals in the times of crisis. The system should allow for quicker than usual approvals in the time of crisis;
- functionality to manage civil carrier movements as part of the military movement;
- functionality to facilitate and to analyse lessons learned from military training operations between the countries.

(5) Information hierarchy:



(6) Operational layout:



- *Each sub-category may be requested separately under the frame of mission request*
- *POC for each sub-category will be according to each member state preference*

Expected impact

- Improved efficiency and speed of the exchange of information related to military mobility. Hence, increased security of the EU Member States.
- Simplification and harmonisation between the EU Member States of the military mobility related information and improved interoperability.
- Enabler for achieving simplified and standardised rules and procedures by no later than 2024 as agreed by the Member States.
- Increased practical cooperation between the EU and NATO on military mobility, which is a flagship area of cooperation between the two organisations.
- Enhanced crisis response and crisis management.

2.18. Call EDF-2021-NAVAL-R: Smart ships

Proposals are invited against any of the following topics:

- **EDF-2021-NAVAL-R-DSSDA:** Digital ship and ship digital architecture;
- **EDF-2021-NAVAL-R-SSHM:** Ship Structural Health Monitoring.

Budget

The Union is considering a contribution of up to EUR 43 500 000 to support proposals addressing any of the above mentioned topics and their associated specific challenge, scope, targeted activities and functional requirements, while considering a contribution of up to:

- EUR 29 000 000 to support an individual proposal addressing the topic EDF-2021-NAVAL-R-DSSDA;
- EUR 14 500 000 to support an individual proposal addressing the topic EDF-2021-NAVAL-R-SSHM.

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

2.18.1. Topic EDF-2021-NAVAL-R-DSSDA: Digital ship and ship digital architecture

Digital technologies evolve at a very high pace, with civilian markets as key driver for innovation. The mastery of the data cycle, from capture to management and exploitation, is now considered as a key element for ship superiority at sea (combat capabilities, improved maintenance, enhanced crew training…). To ensure the adequate integration of innovative digital capabilities and the development of advanced data-based services, it is necessary to define a data-centric IT infrastructure, based on principles that offer resilience, high level of native security, availability and performance as well as computing and storage scalability – while considering the specific requirements of European navies (duration of the mission at sea, low connectivity, sea conditions and environment, interoperability…). This topic is a structuring one. It aims to help the development of fundamentals for digital ship: digital architecture and data/interface standards and ask for the studies of a concrete demonstration on ship and ship systems health monitoring.

Specific challenge

The specific challenge is directed towards the definition of shared digital architecture of naval surface vessels and data/interface standards, against which innovative data management solutions will be tested and selected. This architecture will in particular include a modelling and simulation environment (including digital twinning) that allows for intelligent predictive maintenance based on sensor technology, crew training, training, continuous upgrades of naval capabilities and on-board assessment of the impact of degraded systems on critical functions and ship capabilities, assisted by on-shore experts. A model-based systems engineering design approach that represents a realistic testing environment for the continuous integration of evolving digital technologies (processing, data storage capacities, Industrial Internet of Things (IoT)…) to ensure the openness and scalability of ships' digital architecture.

Strategic importance is identified as the overarching goal to increase the level of automation and support to the ship crew in order to be able to reduce the crew, obtain higher speed in the OODA-loop (observe–orient–decide–act), ensuring high value military tasks, increase safety, operational efficiency, operational readiness (training on real data) as well as decreasing the total life cycle cost of the ship.

Scope

The proposals must aim at obtaining higher degrees of automation in ship and combat systems using big data analysis, data fusion, Artificial Intelligence (AI), including machine learning and multi-agent technology and other technologies to obtain higher speed in the OODA loop, including digital twinning. This objective will be achieved through the definition of a data-centric digital architecture and shared data/interface standards, allowing for new services.

The proposals must address some of the following elements:

- identification of the specifications for warships' digital architecture such as European navy needs and specific constraints (operational, environmental, energy-related, connectivity-related…);
- definition of a ship digital architecture and of smart processes in order to optimise sharing, pushing, pulling, selection, collect, enrichment, exploitation of data, whether for optimising the functioning of systems or for constituting data bases of knowledge or data bases for machine learning or both;
- development of a limited set of interface and implementation standards in order to ensure interoperability and the integration of future data-based solutions and services in various ships.
- a modelling and simulation environment based on Model-Based Systems Engineering (MBSE) principles;
- the combination of IoT technologies, sensors, data lake infrastructures to improve data collection and management, and AI-based analysis capabilities to be able to provide services as to assess a platform's health status and develop predictive and corrective maintenance strategies;

- the capability to introduce novel technology or functionality on an existing design and demonstrate impact on Requirements, Functional, Logical and physical domains;
- the definition of the best application of digital twinning aiming both at product development and lifecycle management.

Targeted activities

The proposals must cover the following activities as referred in Article 10(3) of the EDF Regulation, not excluding possible upstream activities eligible for research actions if deemed useful to reach the objectives:

- studies, such as feasibility studies to explore the feasibility of new or improved technologies, products, processes, services and solutions;
- the design of a defence product, tangible or intangible component or technology as well as the definition of the technical specifications on which such design has been developed which may include partial tests for risk reduction in an industrial or representative environment.

The targeted activities must in particular include:

- definition and demonstration of principles for implementation of a standardised on-board naval IT infrastructure, which may integrate computing, storage, networking, and virtualization resources to be able to run on commodity hardware and/or withstand country-specific choices of technical solutions, but also standards to allow for the joint development of new services and data-based solutions;
- identification, evaluation, test and selection of classes of solutions/services to address data management issues of data integrity, data and user's confidentiality and data traceability;
- MBSE implementation in existing design environment. Availability of physical-mathematical models for system behaviour;
- select and design new (AI-based) functionalities aiming at increasing the level of automation and support for operational crew on-board, increasing the efficiency and effectiveness of the OODA loop;
- SPDM (simulation process and data management) and PLM (product life cycle management) integration for platform and combat system development;
- Industrial IoT standards, data infrastructure solutions and AI-based algorithms. Component and system failure modelling;
- modular design principles to reduce interfaces among systems and facilitate upgradability of system.

Definition and demonstration of ship and ship systems health monitoring:

- design, development and realization of an engineering environment using MBSE for the design of 2 to 5 complete systems (*e.g.* power and propulsion system, pumps, heating, ventilation and air conditioning (HVAC) system, combat system capability);

- definition of a model-based systems engineering design approach that represents the ships' functions and capabilities for advising the crew on remaining functions and capabilities if systems are degraded;
- design of a condition monitoring method for selected systems and develop component and system failure models. Development of AI- and/or physics-of-failure- based algorithms to predict remaining useful life of critical components. Development of AI-based algorithms to predict remaining critical functions and ship capabilities in case of damage, failure or anomalies;
- implementation of modular design principles in a state-of-the-art IT-architecture to be able to upgrade and or to replace components or part of systems and assess impact on requirements, functional performance, logical architecture and physical integration.

A detailed planning of potential subsequent phases must be generated, including the identification of implementation priorities, according to the operational needs.

Functional requirements

The proposals must include a technological demonstrator for the proof of concept. The proposed solution should provide a collaborative environment with the capability:

- to provide and demonstrate a basic functions representative infrastructure framework including all main aspects of storage, processing, communications hardware and protocols, administration and supervision, *etc*. Taking into account the specific constraints and requirements of naval warfare;
- to apply MBSE allowing for the simulation of behaviour modelling while demonstrating impact on requirements, functional, logical and physical domains;
- to demonstrate the design of 2 to 5 systems including physics-based modelling of these systems;
- to demonstrate Industrial IoT technologies, sensors, operator interfaces, data lake infrastructures and AI-based analysis capabilities to be able to assess a platform's health status and develop predictive and corrective maintenance strategies;
- to demonstrate condition monitoring for selected systems and develop component/system failure models, as a demonstration of the service provided by digital ship;
- to demonstrate upgradability by using MBSE and modular design principles and the capability to assess operational effectiveness;
- to demonstrate continuous deployment of (software) systems in the digital twin integrated system environment and on board;
- to demonstrate easiness and effectiveness of adding new functionalities and digital capabilities, without altering the existing system, on the basis of shared standards for data and interfaces.

The digital architecture solutions should comply with the following functional objectives:

- Resilience: to identify architectural principles against undesirable events (*e.g.* combat damages resulting in decreased capabilities, loss of power, cyber-attack, *etc*.) that allow fast recovery, core functions in degraded mode, *etc*.;
- Security: to define and select common architectural principles that maximize security against cyber and physical threats. The safety of the infrastructure for the ship itself is also to be considered;
- Sustainability: focusing both on the ability to maintain the architecture's operational availability at reasonable costs (*e.g.* maintainability, obsolescence management, *etc*.) and as the optimization of resource-usage (*e.g.* lean architecture, energy optimization, *etc*.). The ability of the architecture to evolve and integrate future technologies and architectural patterns is another key aspect of sustainability.

In particular, these solutions should define the optimal allocation of operational functions to systems or subsystems and the mutualisation of hardware capabilities (processing, data storage capacities). To support this optimal allocation, a review and evaluation of digital architecture models currently used in the civilian world is to be conducted against requirements. Models to be evaluated should include cloud computing (Iaas/PaaS/SaaS[76]), edge computing, service-oriented architectures (SOA) or micro-services architectures. Selected infrastructure must offer centralized and mutualized technical services such as management, policies, security, mobility, data collection using IoT technologies, which can be shared by applications and which must contribute to reduced effort in development, shortened time for integration and qualification of incremental capabilities.

For the purpose to seek for interoperability between actions under the two topics considered in this call for proposals, it is encouraged that the proposal addresses possible linkages to the other actions under the topic EDF-2021-NAVAL-R-SSHM (Ship Structural Health Monitoring).

Expected impact

- The definition of a data-centric IT infrastructure to ensure the adequate integration of innovative digital capabilities and the development of advanced data-based services, while considering the specific requirements of European navies, to provide ship superiority at sea.
- The implementation of an MBSE systems of systems digital architecture in a connected environment on-board and on-shore (digital twinning), integrating the various platform's systems will allow for several breakthroughs inter alia, in terms of integrated mission management and systems diagnosis, predictive maintenance facilitating mission planning and mission planning adaptation, simulation and training scenarios, reduced manning and/or autonomous operations.

[76] Infrastructure as a Service/Platform as a Service/Software as a Service.

- The full digitalization combined with the data assimilation of the different sensors will provide safer platforms, increase reliability of equipment and systems, increase endurance and lower maintenance and logistic support cost.
- Establish a collaborative framework for standardization in terms of data and models.
- Facilitate platform adaptability. Facilitate the validation and incorporation of new technologies in the platform during its lifecycle. Navies can remotely configure customized platforms and assess operational effect.
- The possibility to work in cooperation will extend the surveillance and operational capabilities of the platforms.

2.18.2. Topic EDF-2021-NAVAL-R-SSHM: Ship Structural Health Monitoring

Researching on structural health monitoring techniques and their integration in an expert system specific for naval vessels.

Specific challenge

The specific challenge is directed towards the transition from traditional time-based scheduled maintenance schemes to condition-based maintenance (CBM) and complete lifecycle monitoring and management of naval vessels. Such a transition is of paramount importance for reasons associated with reduced maintenance costs, increased operational availability, increased safety, and optimization of operational performance.

Strategic importance is identified as the overarching goal to utilize the big amount of data from sensor measurements by innovative means. When included in the monitoring system, this will offer new information and capabilities on-board and on-shore. Model analysis and tools will further help optimization of design, support the implementation of sensor systems, such as the location and number of sensors, as well as optimize the hull and ship maintenance program. Sensor-based model tools will also be relevant for simulated exercises and training.

Scope

The proposals must aim to obtain improved naval vessels' operational capability through research on advancing the utilization of data from the state of the art, and/or innovatively improve the hull ship structural health monitoring systems, using modern data science tools, such as machine learning, artificial intelligence (AI), digital twin models or other. This will address key topics, such as safe operational envelopes both in peacetime operations and crisis/war situations, weapon systems accuracy improvement, sensors' optimal placement and networking, ship hull structural computational modelling and lifetime extension, damage detection/diagnosis and prognosis, vibration contribution to the hydro-acoustic signature – or more general the vessel’s signatures and condition – and their integration in a decision-making system for naval vessels.

Targeted activities

The proposals must cover the following activities as referred in Article 10(3) of the EDF Regulation, not excluding possible upstream activities eligible for research actions if deemed useful to reach the objectives:

- studies, such as feasibility studies to explore the feasibility of new or improved technologies, products, processes, services and solutions;
- the design of a defence product, tangible or intangible component or technology as well as the definition of the technical specifications on which such design has been developed which may include partial tests for risk reduction in an industrial or representative environment.

The targeted activities must in particular include:

- extension of the on-board SHM systems to detect features in data related to damage detection and assessment, and in that way expand operational envelopes by optimal utilization of vessel capabilities;
- identification of local/global structural vibrations that contribute to the vessel's hydrodynamic signature and establish tools to aid operators in visualization and prediction, with the result of avoid being recognized/positively identified by "red forces";
- exploration of the possibilities in utilizing SHM measurements of local and global hull deformation/vibrations to improve the precision of weapon systems on board the vessel.

A detailed planning of potential subsequent phases must be generated, including the identification of implementation priorities, according to the operational needs.

Functional requirements

The proposed solution must provide a collaborative environment with the capability:

- to detect features in data related to damage detection and assessment, expanding operational envelopes by optimal utilization of vessel capabilities. All the necessary functions for diagnosis, prognosis, and early warning of events on-board the naval vessel enabling necessary functionality should be integrated, to cover variable and potentially challenging operational, loading, and environmental conditions achieving high correct detection rates at low false alarm rates;
- to consider the human element in multi-level data analysis for different and even remote users (vessel's captain or crew, onshore/ naval base maintenance service, fleet management).

The proposals must also include a technological demonstrator for the proof of concept:

- a design of one or more systems including detailed computational (simulation) models to estimate the structural integrity of the ship with correlation capabilities from measured data;
- a physical realisation of one or more of the designed systems including sensor selection and placement, condition monitoring systems, and the possibility for manipulation to

introduce failures. This to demonstrate the concept effectiveness for predictive maintenance;

- a framework/concept/platform for secure on-shore data collection, analysis and reporting of SHM data to the Navy and other units of the European nations' Armed forces;
- the demonstration of the upgradability of the designed systems and its effect on an operation.

For the purpose to seek for interoperability between actions under the two topics considered in this call for proposals, it is encouraged that the proposal addresses possible linkages to the other actions under the topic EDF-2021-NAVAL-R-DSSDA (Digital Ship and Ship Digital Architecture).

Expected impact

- Achieve an incremental and extensive representation of structural aging/damages and detection capabilities.
- Set condition-based maintenance on well-established and feasible criteria.
- Increase the awareness of current fleet's status.
- Provide decision-making support during navigation based on real-time observations for load alleviation as well as failure management.
- Improve design rules for next generation of naval surface vessels through post-processing of data.

2.19. Call EDF-2021-NAVAL-D: Multirole and modular offshore patrol vessel

Naval combat systems and platforms are essential assets to ensure presence where needed, and exercise control and power at sea.

The main objective is to generate a new multirole and modular class of vessels able to increase current navies' capabilities mainly in terms of Maritime Situational Awareness (MSA), Surface Superiority and Power Projection and also to carry out a large spectrum of maritime operations ranging from peacetime and times of crisis actions to wartime operations.

Proposals are invited against the following topic:

- **EDF-2021-NAVAL-D-MMPC:** Modular and multirole patrol corvette

Budget

The Union is considering a contribution of up to EUR 60 000 000 to support proposals addressing the abovementioned topic and its associated specific challenge, scope, targeted activities and functional requirements.

Up to one action may be funded under this call.

2.19.1. Topic EDF-2021-NAVAL-D-MMPC: Modular and multirole patrol corvette

Specific challenge

The ambition of the EU navies is to drastically increase the flexibility of second line vessels in order to conduct a wider range of operations and to make the vessels more suitable to face 21st century challenges and newest constraints and operational requirements to expand the capacities to interoperate and significantly elevate their level of availability and sustainability.

Moreover, the new class of ships needs to be based on a shared baseline, which can be tailored to different national individual requirements.

These goals can be reached at most optimized cost by a new generation of ships defined with a high level of commonality and modularity and taking advantage of a common engineering knowledge base and the large experiences at EU level.

The challenge is to take into account the different requirements from participating Member States and succeed in defining and demonstrate the capacity of building a family of ships which will have a common baseline (reference ship) jointly with some specificities (modularity in design and flexibility in mission) to answer to specific needs from each participating Member States.

Scope

The proposals must aim to:

- define a shared and common set of rules, standards and interfaces applicable to naval architecture and associated systems to improve the industrial cooperation and integration of the European naval companies and Small and Medium Enterprises (SME) and promote common European supply chains;
- create standardized industrial processes and methodologies and increase Member State's joint capability to develop future warships in a reduced amount of time and at most optimized cost, and so contribute to the competitiveness of the European defence industry;
- increase availability through integration of modularity and flexibility in the design of military vessels, and ultimately to generate a new 2500t-3500t class modular vessel able to increase current capabilities of the navies mainly in terms of MSA, Surface Superiority and Power Projection and also carry out a large spectrum of maritime operations ranging from peacetime governmental activities to wartime operations.

Targeted activities

The proposals must cover the following activities as referred in Article 10(3) of the EDF Regulation, not excluding possible upstream activities eligible for development actions if deemed useful to reach the objectives:

- studies, such as feasibility studies to explore the feasibility of new or improved technologies, products, processes, services and solutions;
- the design of a defence product, tangible or intangible component or technology as well as the definition of the technical specifications on which such design has been developed

which may include partial tests for risk reduction in an industrial or representative environment.

The activities must in particular include:

- definition of common methodologies, tools, set of common rules and standards for the studies and construction of the vessel, list of innovative solutions and relevant technological bricks, list of potential EU original equipment manufacturers (OEMs) to be used during the following phases. This phase also includes the definition of standardized interfaces and the study and demonstration of some core technological bricks that are of highest importance for the concept of the vessel;
- concept and feasibility studies for the reference ship and verification of capability to cope with participating Member States/national specific requirements. Definition of flexible and scalable architectures and demonstration they are able to handle the amount of variability of vessel and systems impacted by the participating Member States/national specific requirements. This phase also includes the selection and the definition of the standardized interfaces with the main systems. The feasibility studies will provide several solutions for the reference ship plus specificities (sizing, general arrangement…);
- concept studies and evaluation, in order to elaborate and characterize the main parameters (sizing, general arrangement…) of MMPC solutions for the reference ship and characterization of national variants, and prepare the next detailed design phase for the MMPC.

In order to increase commonality between national variants, and to reduce non-recurring costs, the systems aboard the vessel must have, as much as feasible and economically interesting, standardized functional interfaces to be defined during the first phase of studies.

To allow participating Member States to share capability modules in the flexible areas, the physical and functional interfaces and technologies in those areas must be common. The confirmation of the feasibility of such flexible area will be demonstrated.

A detailed planning of potential subsequent phases should be generated, including the identification of implementation priorities, according to the operational needs.

Functional requirements

The proposed study must include:

- definition of common and jointly agreed naval standards recognized by Classification Societies;
- definition of common agreed operational standards and criteria for all possible matters not subjected to Classification Societies rules;
- definition and demonstration of common set of system engineering tools and methodology to perform the feasibility studies and design (basic and also detailed design in next step of the project) of the reference ship, as well as the specificities;
- definition and demonstration of common standardized integration and testing procedures;

- definition and demonstration of standardized interfaces for flexible areas;
- definition and demonstration of standardized interfaces for main systems or equipment and networks;
- definition and demonstration of common tools (*e.g.* Product lifecycle management) and data exchange processes in order to collaborate between the members of the industrial team and also with the participating Member States;
- definition and demonstration of common production methods for the reference ship and the participating Member States/national variants.

A reference ship constituting the common part of the platform, as well as the definition of specificities responding to the panel of participating Member States requirements must be defined creating a family of ships, being able to:

- cope with common requirements;
- incorporate innovative solutions aiming to increase the overall efficiency of the vessel during her life-span and reduce the adverse effects on environment;
- integrate new technological bricks. These last must be studied and must demonstrate their interest and their performance for this new family of ships. The list of topics to be studied and demonstrated could include, but not limited to the following: active signature management, innovative green systems for propulsion, electrical production, waste management refrigerating gas, capability to deploy multiple UxV, flex zone preparation and handling system, ship data management (secured data centre, virtualization, remote treatment, data analytics…), smart damage management system (innovative detection/fighting system, remote/automated system, crew localization…), design oriented to circular economy (use of materials facilitating green recycling at end of life, solutions to contribute to climate objectives with a target to significantly and globally reduce the ship's gas emissions when compared to a year 2020 state-of-the-art equivalent ship;
- modular concept that favours reconfiguration and modernization throughout useful life;
- contribute to climate objectives with a target to significantly and globally reduce the ship's gas emissions when compared to a year 2020 state-of-the-art equivalent ship.

Expected impact

- Smart interoperable interfaces allowing an easier integration of new systems aboard the vessel and further naval vessels.
- Potential use of disruptive technologies or dual use possible applications through the definition of a new design process
- Design process and solutions oriented to circular economy: use of materials facilitating green recycling at end of life and innovative green systems for propulsion, electrical production, waste management refrigerating gas...

- Reduction of building time, with increased competitiveness and with a widened level of interoperability and standardization to contribute to enhanced surface superiority and increase the EU fleet integration.
- Enhancement of EU's defence industries competitiveness, innovation, efficiency and technological autonomy, facilitating the widening of cross-border cooperation in particular as regards SMEs and Mid-caps.

2.20. Call EDF-2021-DIS-RDIS: Research for disruptive technologies for defence applications

Proposals are invited against any of the following topics:

- **EDF-2021-DIS-RDIS-QSENS:** Quantum technologies;
- **EDF-2021-DIS-RDIS-NLOS:** Non-line-of-sight optical sensors applications;
- **EDF-2021-DIS-RDIS-OTHR**: Over-the-horizon radars applications;
- **EDF-2021-DIS-RDIS-AMD**: New materials and technologies for additive manufactured defence applications.

Targeted type of applicants

Proposals should be submitted by consortia involving at least two eligible entities, as defined in Article 9 of the EDF regulation, which are established in at least two different Member States or associated countries. At least two of these eligible entities established in at least two Member States or associated countries must not, during the whole implementation of the action, be controlled, directly or indirectly, by the same entity, and must not control each other.

Budget

The Union is considering a contribution of up to EUR 60 000 000 to support proposals addressing any of the abovementioned topics and their associated specific challenge, scope, targeted activities and functional requirements.

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

A lump sum approach will be used. For selected projects, the maximum EU contribution will be based on the eligible costs in the requested funding, but actual payments will be conditioned to the completion of work packages. Proposals should include clear descriptions of the proposed criteria to assess work package completion.

2.20.1. Topic EDF-2021-DIS-RDIS-QSENS: Quantum technologies for defence

Quantum sciences have the potential to be a disruptive technology for a wide range of application domains including defence. At the core of this "second quantum revolution" is information: its acquisition (quantum sensors, quantum imaging), its transmission (quantum communications) or its processing (quantum computation).

In the long term, quantum communications or digital superiority by quantum computing are two examples of how quantum technologies can benefit defence applications.

In a shorter term, quantum sensors are expected to play a major role in offering unprecedented advantages in a defence context. Thanks to quantum physics, new sensors are tested in laboratories with precision not achievable before.

Specific challenge

This topic aims to push the undergoing technological effort, taking into account the special requirement of the defence sector.

The possession and deployment of quantum technologies will be a game changer in many application domains, which means that maturing and mastering these technologies is a must for mission superiority, but also competitiveness. Europe and European countries fully engage to support this technological development, but are currently outpaced by other countries especially China and the United States. This topic proposal aims at filling this gap.

Scope

The ambition is to explore and demonstrate quantum technology solutions in mainly three applicative directions, namely:

(1) Positioning, navigation and timing;

(2) Quantum radio frequency sensing;

(3) Quantum optronics sensing.

Developments concerning specific enabling technologies are intended to be included. Indeed, most of enabling technologies exist already in laboratories. They need now to reach the necessary maturity to meet military operation conditions. This may include: compact cryogenic systems for quantum technologies, fast electronic devices for quantum technologies, specific sources of light for quantum technologies, integration of photonic systems.

Quantum radar (based on entangled RF photons, *i.e.* quantum RF illumination) must not be considered in the proposals since preliminary system analysis have shown operational gains only in very specific and reduced domains of applications.

Some activities covered by the proposals could share multiple communalities, for example in terms of enabling technologies, with other quantum domains of applications (*e.g.* communication, encryption). Whilst not being the objective of this call topic, the proposals should elucidate potential benefits of current works for these other quantum domains of applications.

Targeted activities

The proposals must cover the following activities as referred in Article 10(3) of the EDF Regulation, depending on the topics addressed according to the functional requirements:

- activities that aim to create, underpin and improve knowledge, products and technologies, including disruptive technologies for defence, which can achieve significant effects in the area of defence;
- activities that aim to increase interoperability and resilience, including secured production and exchange of data, to master critical defence technologies, to strengthen the security of supply or to enable the effective exploitation of results for defence products and technologies;
- studies, such as feasibility studies to explore the feasibility of new or upgraded products, technologies, processes, services and solutions;
- the design of a defence product, tangible or intangible component or technology as well as the definition of the technical specifications on which such a design has been developed, including any partial tests for risk reduction in an industrial or representative environment

In particular, for each technical area as referred in the functional requirements, the proposals must include some or all of the following activities:

- analysis of the disruptive potential of specific quantum technology capabilities in defence applications;
- analysis of the technical feasibility, requirement specification, trade-offs and concept definition for an operational use case;
- development of a demonstrator system for an operational use case and maturation of quantum technology components;
- performance verification in a relevant environment such as a testbed aircraft or a research vessel;
- analysis of industrialization and technology maturation needs.

Functional requirements

The proposals must include activities regarding at least one the following topics and comply with the related requirements:

(1) Positioning, Navigation and Timing quantum sensors for Defence

High performances atomic clocks

New concepts of atomic clocks could provide orders of magnitude improvements in terms of frequency stability and compactness compared to standard designs. They tend to become SWaP[77] compatible with on-board platform integration and to allow new collaborative combat and measurement schemes, requiring for example the synchronization of multiple platforms in

[77] Size, weight, power.

Global Navigation Satellite System (GNSS) denied, degraded or contested situations. In addition, the impact of clock sources, such as those used to improve the resilience of strategic communication networks or the continuity of essential services, is of high interest, as well as the technical means to distribute such clock signals.

The proposals must address new concepts of atomic clocks significantly improving currently available frequency stability in a compact form factor. Specific developments of enabling technologies such as low-noise laser sources, compact optical benches, photonic integrated circuits and compact atomic vapour cells must also be considered.

Cold atom-based inertial sensors

The use of cold atom interferometers is known to bring disruptive possibilities to develop compact multifunctional inertial measurement units, which have the capacity to drastically improve autonomous navigation. The bandwidth of these sensors will benefit from hybridization with classical accelerometers and gyrometers (*e.g.* MEMS[78] and FOG[79]).

The proposals must demonstrate functionalities such as accelerometry, gyrometry and combination of these functionalities with time measurements to significantly improve autonomous positioning and navigation. Specific developments of enabling technologies such as compact electronics, photonic systems or vacuum systems must also be considered, with the perspective of a SWaP integration of these functions.

Cold atom-based gravimetry

Cold atom-based gravimetry will allow the creation of accurate gravity maps leading to new applications in terrain aided navigation, calibration of inertial measurement units before mission start and higher accuracy gravimetry correction for strap down navigation. These will lead to enhanced capability for autonomous navigation.

The proposals must include activities demonstrating the feasibility of cold atom-based gravimetry for navigation. Specific developments of enabling technology such as compact narrow linewidth lasers and compact vacuum system must also be considered.

Levitated inertial sensors

Optical fields and AC electric field can be used to exert forces on material particles and levitate them in a vacuum environment. These systems can be used as inertial sensors, to probe accelerations, rotations and gravitational fields. Such sensing devices can reach quantum regimes of detection, thus reducing the internal noise of the device.

The proposals must address the possibility of packaging these systems in a sub-centimetre scale, remotely controlling them with optical fibres, and examine the versatility of deployment options, making them a disruptive technology that will allow a new range of military applications.

[78] Microelectromechanical systems.
[79] Fiber Optic Gyro.

Optical fibre inertial sensors

Optical fibre sensors are mechanically robust, lightweight, cheap, totally passive, and immune to electromagnetic interference and can be read out also by km distance with a completely passive operation. Ultra-high bandwidth vibration, acceleration and rotation sensors with sensitivity performance well beyond the state of the art can be developed harnessing cutting-edge laser optical quantum technologies in combination with telecom-grade optical fibre components. Compact interferometric structures relying on optical fibre elements and resonators can be interrogated with non-classical light sources and single-photon detectors.

The proposals must include activities regarding this topic which can lead to systems likely to be disruptive in real-time monitoring of ground movements, residential structures, air/surface vehicles as well as high-precision underwater navigation.

Solid-state quantum vector magnetometers

Solid-state magnetometers based on colour centres in crystals, such as Nitrogen vacancy (NV) centres in diamond, are quantum devices operating at room temperature that offer highly sensitive, compact, and low power-consumption solutions to reconstruct full vector magnetic field maps. These systems can lead to enhanced capabilities in navigation and geo-referencing based on magnetic anomaly maps.

The proposal must address new sensing schemes and concepts for quantum vector magnetometry significantly improving currently available sensitivity and resolution. The development of enabling technologies such as microwave electronics, optical integration techniques, material engineering, imaging methods, readout architectures or signal processing must be considered.

(2) Quantum radio frequency sensing for defence

Quantum Technologies for high sensitivity RF sensing

The proposals must address the potential gain in performance that can be achieved using quantum technologies to sense classical RF illumination.

Quantum systems such as ensembles of atoms in Rydberg state or superconducting quantum devices exploiting interference effects are promising new EM fields sensing schemes offering unprecedented sensitivity and accuracy. These approaches, amongst others, could allow compact antenna or sensing schemes over large frequency bandwidth, exchanging the usual “antenna gain” of classical/large sensors for the gain in sensitivity provided by compact and potentially covert quantum-based devices. The proposal must include activities regarding this topic.

All dielectric, highly compact and intrinsically calibrated ultra-wideband (MHz-THz) RF field sensors can be envisaged for instance with Rydberg atoms at room temperature. To demonstrate their practical implementations and performances compared to standard antennas, the proposal must investigate optimized optical excitation and interrogation schemes, in parallel with enabling technologies such as frequency controlled laser sources at specific wavelengths, compact atomic vapour cells and optical integration techniques.

Superconductive devices based on Josephson Junctions have proved astonishing level of sensitivity even at temperature >30K, which makes them solid candidates for both magnetic anomaly detection and sensor applications where miniaturized antennas with high performance are required. In this domain, it is necessary to optimize technological features in order to reach reliable wafer-scale fabrication process. The proposal must include activities demonstrating the feasibility of such detectors and showing their superiority over current detectors. As an enabling technology, the development of compact cryogenic solutions must also be considered.

Quantum Technologies for electronic intelligence (ELINT)

Quantum sensing offers unique opportunities for electromagnetic landscape monitoring and ELINT. NV centres in diamond and more generally colour centres in crystals could allow the realization of compact solid-state spectrum analysers or RF signal classification schemes covering most of the radar frequencies and working at room temperature. Improving their performances requires enhanced sensing schemes and concepts, high quality material, optimized RF antenna, controlled magnetic field, low noise optical detection.

The proposals must include activities demonstrating the feasibility of such detectors and showing their superiority over current detectors. The development of several enabling technologies such as material engineering, microwave electronics, optical integration techniques, optimized imaging methods, new signal reading architectures or signal processing must also be considered in order to achieve compact sensors with optimized performances for ELINT.

(3) Quantum optronics sensing for Defence

Active systems based on non-classical illumination

The proposals must address both quantum illumination with entangled photons (*e.g.* quantum LIDAR[80]) and more generally exploitation of quantum technologies for optronics sensing and imaging.

Multiple quantum imaging schemes have been proposed to improve the performances of active optronics remote sensing systems in terms of sensitivity, covertness and hacking/jamming robustness, and also to offer the capability to operate in poor propagation conditions and Degraded Visual Environment (fog, rain…).

The proposals must investigate their impact on operational capabilities and their practical implementation. Examples of schemes to be explored include quantum ghost imaging (QGI) and quantum LIDAR based on entangled photons sources, 2D/3D imaging based on single photon array detectors, broadband multispectral sensor… Specific developments in enabling technologies must also be considered, including for example single photon bucket detector, high resolution and gated single photon array detectors (SPAD), efficient entangled photon

[80] Light detection and ranging.

sources for QGI and quantum LIDAR, graphene and quantum dot for visible and infrared light sensors, quantum detectors/modulators (QWIP[81], QCD[82],…).

Passive systems based on Quantum Technologies

Passive systems for optronics sensing could also benefit from quantum technologies. In analogy to RF sensing, passive optronics systems can be improved both in terms of sensitivity and of functionalities, harnessing devices and concepts based on conventional photo-switch quantum technology-based devices and concepts.

Examples of schemes to be explored by the proposal include: photon statistical analysis (analogous to the Hanbury Brown and Twiss effect) and thermal ghost imaging, ghost Mach-Zehnder interferometry, and more generally coherent detection of thermal photons. Such schemes are expected to provide additional or improved capabilities such as lens less ghost imaging, increased spatial resolution for thermal imaging, optical imaging/detection of phase objects, and imaging/detection of gas (leaks or CBRN[83]). Specific developments in enabling technologies must also be considered, including single photon bucket detector, SPAD, QWIP/QCDs, MEMS-based optical sensors, low noise/large coherence QCLs[84]/ICLs[85].

Expected impact

- Efficient GNSS-free navigation based on quantum inertial sensors, anomaly mapping and reliable micro-atomic clocks.
- Innovative and accurate quantum enhanced RF sensors operating in a defence context.
- Innovative and accurate quantum optronics sensors and imaging systems operating in a defence context.
- Development of EU supply chains for specific enabling technologies that are considered essential to master the overall capability.

2.20.2. Topic EDF-2021-DIS-RDIS-NLOS: Non-line-of-sight optical sensors applications

Optical technologies are facing a paradigm shift by an evolutionary revolution from digital imaging to computational and quantum imaging. These disruptive novel optical sensing approaches could bring game-changing sensing capabilities to many military operations. As a lighthouse technology in computational and quantum imaging indeed, non-line-of-sight imaging (NLOS) could overcome limitations of classical optical sensing which are tied to the direct line-of-sight, as it can extend the perception range of an optical sensor to areas hidden from direct view, while insuring high spatial optical resolution. In the future, this emerging technology might therefore enhance soldier's observation and detection capabilities dramatically by bringing imaging and ranging capabilities, in many operational scenarios where current technologies such as line-of-sight optical sensing or RADAR fail to deliver

[81] Quantum well infrared photodetectors.
[82] Quantum cascade detectors.
[83] Chemical, biological, radiological and nuclear.
[84] Quantum cascade lasers.
[85] Interband cascade lasers.

relevant data with appropriate resolution. Possible operation scenarios include enhanced situational awareness, mission planning for hostage rescue (localization of persons in building) and threat analysis like detection of ambush.

Specific challenge

This topic aims to push the development of novel quantum sensing devices, laser technologies and computational algorithms such as geometrical reconstruction and artificial intelligence, such as to enable a breakthrough in optical sensing and situational awareness.

Classically, the perception area of optical sensors is limited to the line-of-sight. This area can be extended by computational imaging to areas outside the direct line-of-sight: using highly sensitive devices, multiple diffuse reflected photons can be recorded and their signatures analysed by sophisticated algorithms, such as physically based back-projection or artificial intelligence. Due to multiple diffuse reflections, the expected signals are very low and require quantum sensing devices with single photon counting capabilities. Further, the sensors have to measure the photon roundtrip path length with high precision.

Scope

Expertise from different fields is to be combined to build a demonstrator to be validated in a relevant environment. In this context, the topic calls for research in fields of computer science, for the development of novel reconstruction algorithms, semiconductor electronics, for the development of highly sensitive and precise single photon counting devices, and photonics for the development of laser illumination and optical receiver. All research activities may be led to a laboratory scale demonstration system which may be tested in relevant scenarios.

Targeted activities

The proposals must cover the following activities as referred in Article 10(3) of the EDF Regulation:

- activities that aim to create, underpin and improve knowledge, products and technologies, including disruptive technologies for defence, which can achieve significant effects in the area of defence;
- activities that aim to increase interoperability and resilience, including secured production and exchange of data, to master critical defence technologies, to strengthen the security of supply or to enable the effective exploitation of results for defence products and technologies;
- studies, such as feasibility studies to explore the feasibility of new or upgraded products, technologies, processes, services and solutions.

The proposals should support the development of novel sensor devices dedicated of NLOS sensing, the development of new reconstruction algorithms with the aim of fast reconstruction of the hidden scene, the development of a compact laser source with performance adapted to the specific needs of NLOS sensing and the development of a laboratory system to investigate and demonstrate NLOS sensing in relevant scenarios.

An integrated experimental setup is expected with first approaches for self-calibration and self-adoption to environmental conditions within the first 3 years. Then the maturity must be increased by further integration of the system components (laser, sensor, optics, software) and investigate first relevant scenarios by testing in representative environment.

The proposals must finally give prediction on how the technology investigated could be integrated into military sensing platforms and industrial products.

Functional requirements

The proposals must fulfil the following requirements:

- combine appropriate photon-counting sensing devices and computational imaging analysis to sense and reconstruct the NLOS scenario;
- be able to self-calibrate the 3D LOS scenario, which is a prerequisite knowledge to reconstruct the NLOS scenario;
- define a modular approach in order to explore different sensing layouts, system designs and to evaluate their performances (single-pixel or array sensor, single laser point illumination or scanning illumination);
- increase the maturity level of an NLOS system from generating and integrating knowledge to study in a 5-year time scale. The aim is to test the system in representative environment in a static or dynamic scenario closer to later use in military operation;
- develop a thorough model for NLOS scenarios, able to reliably simulate performances (resolution, SNR[86] …) of the system as a function of the experimental parameters such as distance, chosen operating wavelength, background noise level, system efficiency, hidden object dimensions, atmospheric effects, dark counts and gating effects;
- improve the development of sensor and laser technology in order to increase NLOS performances (sensor sensitivity and time-resolution, laser power and pulse duration);
- develop fast data analysis algorithms to tackle real-time capabilities or, at least, reconstruct a distant NLOS scenario (several meters round trip) on an appropriate time scale (less-than-a-minute time scale);
- establish a laboratory testing scenario of a hidden-scene to evaluate the performance of NLOS sensing systems and reconstruction algorithms;
- increase the stealth and eye safety of NLOS systems by shifting the illumination wavelength from the VIS[87] spectrum to SWIR[88] spectrum;
- define and establish a military relevant testing scenario to demonstrate the potential use of NLOS technology.

[86] Signal-to-noise ratio.
[87] Visible.
[88] Short-wave infrared.

Expected impact

NLOS sensing will change the way how we think about optical sensing, and will bring new sensing capabilities that might increase the situational awareness and observation capabilities of the soldier dramatically, and therefore increase survivability and the superiority of own troops. In this perspective, NLOS sensing is expecting to strongly impact military operations.

The technology will enable new optical imaging and ranging within a hidden scene without direct line-of-sight, including being able to "look around corners". This technology might be used in many operations where information about a hidden area is needed but beyond direct access. Possible operation scenarios include enhanced situational awareness, mission planning for hostage rescue (localization of persons in building) and threat analysis like detection of ambush.

Disruptive progress in quantum sensing devices is expected to bring game-changing capabilities in light sensing with high-dynamic range from daylight to very low light conditions. In the area of reconstruction algorithms, breakthrough in analysis is expected with a three dimensional resolution in real time, at performance levels close to current line-of-sight sensing. These reconstruction algorithms could also advance and push developments in current side technologies such as noise removal or viewing through turbid media (*e.g.* brownout, submarine).

2.20.3. Topic EDF-2021-DIS-RDIS-OTHR: Over-the-horizon radars applications

The EU requirements for surveillance, as depicted in the 2018 capability development plan, describe the necessity for increased situational awareness through means such as long-range radar systems. In that sense HF (High Frequency) Over the Horizon radars can be a viable solution that offers target detection over very long-range by exploiting propagation characteristics of HF waves. This can be distances in the order of thousands of kilometres by using the sky waves, which are reflected down from the ionosphere, or some hundreds of kilometres by using surface waves, which follow the earth curvature. However, sky wave radars have an extensive blind area (the skip distance) because the sky waves reflect down to earth at distances beyond 1,000km and thus leave areas at shorter ranges without illumination.

For the reasons stated above, such installations are well suited to countries occupying a large area, particularly because of the zone of about 1,000km radius extending the radar transmitter which is not covered by sky-wave propagation. USA, Russia, and Australia among others have already developed OTH radars and have the ability to monitor such large areas. For geographically confined countries though, collaborative air and maritime picture over large areas can be acquired only through a cooperation among them that will utilize OTH radar units operating in a networked environment. Thus, this technology scale naturally fits the extent of the European continent and requires collaboration between Member States to improve collective defence and situational awareness.

Specific challenge

The specific challenge of this topic is to address new technologies to be developed by integrating different HF infrastructures (transmitters and receivers) in a collaborative and passive mode to increase air and sea detection range. That includes:

- collaborative and passive OTH Radar networking;
- ionospheric sounding network to monitor the status of the ionosphere interacting with OTH radar;
- non-cooperative broadcasting HF emitters as illuminators of opportunity;
- cognitive spectrum management and algorithms to detect challenging targets.

Scope

To enhance situational awareness and operation superiority, there is an EU requirement to improve detection, tracking and identification capabilities over wide areas and with minimum latency. High frequency over-the-horizon systems need therefore to be improved whilst an EU concept for cognitive and scalable network, both active and passive, of HF OTH sensors could be investigated.

This topic addresses the technologies for EU OTH radar concept offering deep collaborative strategic surveillance and data sharing. In this regard, both HF Surface- and Sky- Wave radar technologies should be explored regarding their respective advantages in terms of covered area in long ranges and as a gap filler.

Targeted activities

The proposals must cover the following activities as referred in Article 10(3) of the EDF Regulation, not excluding upstream activities eligible for research actions if deemed useful to reach the objectives:

- activities that aim to increase interoperability and resilience, including secured production and exchange of data, to master critical defence technologies, to strengthen the security of supply or to enable the effective exploitation of results for defence products and technologies;
- studies, such as feasibility studies to explore the feasibility of new or upgraded products, technologies, processes, services and solutions;
- the design of a defence product, tangible or intangible component or technology as well as the definition of the technical specifications on which such a design has been developed, including any partial tests for risk reduction in an industrial or representative environment.

The proposals must conclude to the creation of a proof of concept for the intended solution. This will exhibit the intended functionality and act as a testbed for the development of prototype-scale projects in the future.

The targeted activities should in particular include:

(1) Integrating knowledge

- review of defence requirements and accordingly define the preliminary CONOPS for the OTH radars;
- definition of OTH Radar specifications based on preliminary CONOPS coming from the end users (armed forces of involved EU members). These should cover collaborative air space and maritime surveillance;

(2) Studies

- new signal processing techniques, among others, for:
  - clutter mitigation;
  - improving target localization and tracking;
  - Multiple Input Multiple Output (MIMO) configuration;
- reduction/use of multipath and Doppler fading;
- study of the very long baseline related issues:
  - synchronization of installations;
  - direct signal disturbance mitigation;
  - usage of passive mode by exploiting (non-)cooperative illuminators in HF band.

Furthermore, activities specifically targeted on HF Sky-wave radars should include:

- support for multiple radar configurations for better footprint management (*e.g.* one remote illuminator/multiple reception sites or multiple remote illuminator/multiple reception sites);
- focus on receiver architectures, mainly oriented to SDR technology;
- focus on transmitter technologies, particularly on power amplifier architectures;
- signal waveforms and coding;
- novel antenna element designs, array architectures and/or scanning techniques;

(3) Design

- real time atmospheric propagation models based on processing of data collected by a network of sensors, such as advanced ionosphere stratification models;
- new techniques for optimized use of electromagnetic spectrum management (frequencies and bandwidth);
- new signal processing techniques, among others, for:
  - clutter mitigation;
  - improving tracking capabilities and target localization;

- multistatic system combinations and Multiple Input Multiple Output (MIMO) configuration.

The abovementioned technologies should be demonstrated (partially or in whole) through small scale or reduced functionality (*e.g.* shorter antennas, reduced power, *etc*.) technology demonstrators. Modularity in terms of future expansion towards a prototype and use of existing equipment / infrastructures must have positive consideration. Additionally, EU technology should be incorporated to the greatest possible extent.

Functional requirements

The proposals must fulfil the following requirements:

- operate at long over-the-horizon ranges, far beyond current existing systems, to detect and track air and sea targets such as large aircrafts and ships moving at speed of more than 25 kts;
- fill the gaps and extend current air and sea EU radar surveillance coverage, using a collaborative network of sensors and the necessary synchronization;
- implement advanced ionospheric sounding networks and validated models in order to operate cognitive radar management schemes for radar network operation;
- implement advanced signal processing to improve OTH detection and tracking performances and target localization.

Expected impact

- Development of the necessary infrastructure to the participant Member States for making them capable to pursue research and development in the OTH Radar field.
- Incorporation of ionospheric propagation models for supporting the radar in real-time.
- Collaborative operational exploitation of the networked OTH radars (active and passive).
- Instigation of future research projects in the topics of detecting extra-atmospheric and/or hypersonic objects.
- Strengthening the European industrial and technology base by identifying critical components and units.
- Strengthening the collaboration among industries and research institutes.

2.20.4. Topic EDF-2021-DIS-RDIS-AMD: New materials and technologies for additive manufactured defence applications

Additive manufacturing (AM) allows producing multi-functional parts and has been introduced into various industry segments over the last decade. For future military applications employing materials that are even more advanced, the AM process still requires significant technology development in order to establish robust and high yield processes to tap its full potential. The complexity of the necessary processes of additive manufacturing requires a profound understanding of material chemistry, metallurgical structures on microstructural level as well as defect detection on the macroscopic level. Research

activities [89] could include but are not limited to identification and analysis of material properties, such as (super)alloys or concrete composites, full functional 3D printed electrified structures, new technologies to further improve military propulsion, AM parts or structures for an improved protection of soldiers and equipment, specialized AM-materials for function and structure in next-gen ammunition and missiles or AM technologies for ballistic functional structures as well as new approaches to lightweight applications.

Specific challenge

Additive manufacturing (AM) allows production of parts for various defence-industries segments with various technologies and materials. AM can, for instance, improve development processes due to shorter production times, manufacture obsolete spare parts or parts on-demand, or produce parts with integrated functions or parts of high complexity. There are several topics related to AM that can be addressed in research activities. These activities could include but not be limited to: the identification and analysis of material properties, such as (super)alloys or concrete composites, full functional 3D printed electrified structures, specialized AM-materials for advanced ammunition and missiles or AM technologies for ballistic functional structures.

Proposals should in particular address R&T efforts in the areas of:

- identification and analysis of new materials for AM for defence application;
- innovative AM technologies and procedures, *e.g.* for the production of multi-functional parts.

Proposals should address R&T in one or more of the following areas:

A Additive Manufactured Electronics (AME)

In order to overcome future challenges in defence electronics, the aspects of increased miniaturisation and complexity is of major importance. Furthermore, SWaP-C needs to be considered, too. In case of damage, defence electronics should be replaced as soon as possible and not depend of the availability of spare parts. Therefore, the impact of supply chain management and their impact to the independency from outer EU regions is vital. Finally, classical manufacturing of PCBs is related to significant numbers of harmful substances, like acids or galvanic fluids. This is directly related to RoHS and REACH requirements.

B Additive Manufacturing of Advanced Ammunition

For the next generation of ammunition several challenges need to be addressed, *e.g.* increased performance, improved reliability and safety, additional functionality, changing requirements and adequate supply. AM can be used to produce ammunition covering both, the production of the body/shell and the high-energetic material. The high degree of freedom in shape, can led to significant improvements in performance as the ammunition can be designed and adopted to several mission-specific requirements. For example, pressure profile in a barrel can

[89] Materials and products have to be as Safe and Sustainable as possible By Design and during their life cycle (COM(2020) 667 final - Chemicals Strategy for Sustainability; Towards a Toxic-Free Environment, COM(2021) 400 final - Pathway to a Healthy Planet for All; EU Action Plan: 'Towards Zero Pollution for Air, Water and Soil').

be improved by the design of the energetic-material or the fragmentation of a shell can be influenced by the shape of the casing.

C Additive Manufacturing for Protection

Different groups of additive manufacturing technologies provide the opportunity to improve the protection of soldiers and equipment by advanced approaches to avoid or resist threats. Using the flexibility in terms of shape and complexity, AM parts or structures can be manufactured without the restriction of classical technological limits. Particularly for resistance it is important to absorb energy and withstand high-strain rates, where AM structures can show an improved protection quality and/or reduced weight.

D Additive Manufacturing for Lightweight Structural Parts

Lightweight structures can be achieved through a geometrical lightweight design and/or the use of lightweight material. AM offers the opportunity to address both by taking advantage of the freedom in the shape using (new) lightweight materials leading. Additionally, using AM for structural parts leads to the necessity of safe and robust processes leading to high-quality products.

Scope

Proposals should consider the current state-of-the-art including additive manufacturing systems, materials and material properties. Additionally, the entire additive manufacturing process should be taken into account in order to evaluate and classify the planned activities within a project.

Proposals are generally intended:

- to improve the understanding of the investigated AM-processes;
- to further develop the manufacturing technology;
- to evaluate the potential compared to other solutions;
- to improve the performance of the products, processes or operations addressed by the proposal.

For the previously mentioned areas, this means:

A Additive Manufactured Electronics (AME)

- to increase the level of integration regarding electronics and RF-components, multiple physical functions should be integrated in multi-functional parts using AM, *e.g.* mechanical, thermal and especially the electric function;
- due to the potential design freedom AME can merge mechanical and electrical functions in one multifunctional structure. Future designs could handle concurrent requirements regarding weight reduction, increased complexity, rapid manufacturing and reduced environmental impact;
- challenging factors to get AME in use at defence level are manufacturing process maturity, definition of material properties and population technologies (*e.g.* soldering, multi-layering). Additionally the ability to create these functional designs is equally important.

Therefore, the education of engineers and definition of design guidelines are therefore the key to implement AME successfully.

B Additive Manufacturing of Advanced Ammunition

- different types of ammunition may be investigated *e.g.* kinetic projectiles, shaped charges, grenades or high and hypervelocity ammunition. The specialized materials must be characterized and tested with respect to their intended use, *e.g.* high-density materials needed for kinetic projectiles;
- to improve and adopt the behaviour of ammunition items energetic materials may be additively manufactured to affect the time-dependent energy conversion. To affect fragmentation gradients in the material properties within a shell may be investigated as well as a complex design of ammunition bodies/shells. To affect propulsion, complex shaped propellant grains may be investigated;
- the quality and accuracy of the AM-process and the AM-processed materials should receive special attention.

C Additive Manufacturing for Protection

- to increase protection different combinations of materials and technologies may be used at each stage of manufacturing process. Different densities, internals structures of components should be considered here, *e.g.* to optimize the protection quality /mass ratio. AM may be used to exclusively manufacture or just perform the modifications of the existing parts. Multimateriality and multifunctionality of the parts may be additionally implemented.

D Additive Manufacturing for Lightweight Structural Parts

- lightweight structures are to be realized addressing both aspects, an optimal distribution of the material as well as improved (weigh-specific) material properties. Therefore, complex designs are to be addressed as well as the use of new materials. Due to the typically low safety factors used for many lightweight applications, special attention should be paid to process and material quality as well as an substantial database, which should be built up for the processed materials.

Targeted activities

The proposals must cover the following activities as referred in Article 10(3) of the EDF Regulation, depending on the topics addressed according to the functional requirements:

- activities that aim to create, underpin and improve knowledge, products and technologies, including disruptive technologies for defence, which can achieve significant effects in the area of defence.

In order to overcome the aforementioned challenges, projects should include the following activities (if applicable):

- analysis of available printing technologies and materials in terms of chemical, environmental, mechanical and thermal properties of the additive manufactured parts;

- investigations on long-term behaviour and effects of environmental conditions;
- analysis of parameters and variables affecting the additive manufacturing process;
- investigations at specimen, sub-component and component level;
- investigations on post-processing and post-treatment of printed parts;
- optimization methods and numerical simulations;
- consideration of testing methods (including non-destructive testing);
- consideration of reliability and quality related issues;
- investigations regarding the overall added value for defence systems and products.

For the previously mentioned areas, target activities additionally must include:

A Additive Manufactured Electronics (AME)

- analysis of material in terms of electrical and RF properties;
- investigations on assembling technologies, *e.g.* soldering, gluing, beam welding and wire-bonding;
- investigations on new possibilities of three-dimensional routing for electronic parts, integrated shielding and increased packing density of RF structures;
- investigations on the integration of microelectronic components and analysis of thermal management;
- investigations to optimize post-treatment processes, *e.g.* to reduce post-treatment temperature;

B Additive Manufacturing of Advanced Ammunition

- analysis of specialized materials (or material-combinations) with respect to the intended use of the ammunition, *e.g.* high-strain-rate or shock driven processes;
- investigation on the performance of additively manufactured ammunition;

C Additive Manufacturing for Protection

- analysis of the material properties and high-dynamic loads and the energy absorbance;
- investigations covering complex or adopted shapes and/or lattice structures;
- ballistic tests of the fabricated resistance structures and components;

D Additive Manufacturing for Lightweight Structural Parts

- investigations on the lightweight potential using optimized designs;
- investigations on the lightweight potential using new material;
- analysis of the process robustness and quality of printed parts during the product life cycle.

The proposals must substantiate synergies and complementarity with foreseen, ongoing or completed activities in the field of AM, notably through EU funded actions under Horizon 2020 and Horizon Europe or in the framework of the European Defence Agency.

Functional requirements

The proposed solutions should include in general:

- build-up and strengthening of European capabilities and resources for equipment and devices related to the additive manufacturing processes;
- proof of concept of the investigated issues on a technology-demonstrator level;
- proof of concept including environmental effects;
- evaluation of the material properties of additively manufactured material on specimen level;
- establishment of a quality-assured AM process chain, including the evaluation of key influencing factors.

For the previously mentioned areas, the proposed solutions additionally must fulfil the following requirements:

A Additive Manufactured Electronics (AME)

- characterization of electronic properties *e.g.* conductivity and proven RF performance *e.g.* microstrip lines;
- established design guidelines for AMEs, *e.g.* conductors, including 3D-routing;
- integrated and assembled generic electronic structure, including microelectronic structures proven on demonstrator level including environmental tests and analyses;
- proof of concept for 3D-routing including integrated shielding with high packing density of electronics components and thermal management using integrated thermal structures;

B Additive Manufacturing of Advanced Ammunition

- proof of concept for ammunition with an additively manufactured body/case and/or energetic material;
- proof of concept for design, *e.g.* fragmentation;
- evaluation of safety aspects related to AM of energetic materials;

C Additive Manufacturing for Protection

- characterisation of mechanical properties for high strain rates and shock loadings;
- improved protection level and/or reduced weight;
- proven protection level *e.g.* acc. to STANAG 2280 (if applicable);

D Additive Manufacturing for Lightweight Structural Parts

- evaluation of lightweight potential due to optimized design and/or new material;
- proven recommendations/ derivations regarding certification aspects for safety-critical parts;
- evaluation of NDT and embedded sensors for health monitoring methods, during production and parts life cycle.

Expected impact

In principle the TRL of the technologies will be increased towards usability in defence applications. Improved performance must be achieved by the manufacture of products that were not possible with classical manufacturing technologies. Additionally, more flexibility is created by reduced effort to implement adaptations and by allowing more flexibility in the place and time of manufacture.

For the previously mentioned sub-topics, in particular:

A Additive Manufactured Electronics (AME)

More and different functions can be combined in smaller volumes. Thus, the integration level of electronic assemblies can be significantly improved. Furthermore, new AME technologies offer a reduced ecological impact, allow on-demand production and reduce the dependence on international supply chains.

B Additive manufacturing of Advanced Ammunition

Ammunition will be more flexible and adapted to mission-specific requirements. Scalability will be improved and raw materials as well as resources can be used more efficiently towards a more time-demand-orientated production progress and reduced environmental impact.

C Additive Manufacturing for Protection

The safety of the soldiers will be improved by an advanced protection of persons, systems and/or infrastructure. Improved protection would directly translate to improved resilience and survivability in missions.

D Additive Manufacturing for Lightweight Structural Parts

Improvements in lightweight design affects to overall performance due to improved agility and speed. Additionally weight reduction will lead to a stress reduction and (for systems) will also reduce environmental footprint.

2.21. Call EDF-2021-OPEN-RDIS: Open call addressing disruptive technologies for defence

The development of new defence products and services very often relies on incremental improvements of existing ones leading to a higher performance or more efficient operation of established capabilities. However, technologies are emerging that could – when used in a military context – radically change the balance of military power between opponents. Such disruptive technologies for defence then lead to game-changing shifts in military paradigms. Exploring innovative technologies for defence use is thus essential to alter or maintain technological dominance.

Proposals are invited against the following topic:

- **EDF-2021-OPEN-RDIS-OPEN:** Research on disruptive technologies for defence

Targeted type of applicants

Proposals should be submitted by consortia involving at least two eligible entities, as defined in Article 9 of the EDF regulation, which are established in at least two different Member States or associated countries. At least two of these eligible entities established in at least two Member States or associated countries must not, during the whole implementation of the action, be controlled, directly or indirectly, by the same entity, and must not control each other.

Budget

The Union is considering a contribution of up to EUR 10 000 000 to support proposals addressing any subject of interest for defence.

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

2.21.1. Topic EDF-2021-OPEN-RDIS-OPEN: Research on disruptive technologies for defence

Specific challenge

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

Scope

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

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

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

Targeted activities

The proposed actions should aim to create, underpin and improve disruptive technologies that can achieve significant effects in the area of defence (generating knowledge), not excluding downstream eligible activities for research actions (integration of knowledge, studies and design).

Functional requirements

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

Expected impact

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

Funding information

The requested funding should match the ambition of the proposed action and be duly justified. In any case, the requested funding should not exceed EUR 4 000 000.

A lump sum approach will be used. For selected projects, the maximum EU contribution will be based on the eligible costs in the requested funding, but actual payments will be conditioned to the completion of work packages. Proposals should include clear descriptions of the proposed criteria to assess work package completion.

2.22. Call EDF-2021-OPEN-R: Open call focused on SMEs for research on innovative and future-oriented defence solutions

Research on innovative and future-oriented defence products and technologies significantly relies on the innovation capacity of Small and Medium-sized Enterprises (SMEs). This call for proposals is focused on SMEs and targets research on any innovative defence products, solutions and technologies.

Proposals are invited against the following topic:

- **EDF-2021-OPEN-R-SME:** Research on innovative and future-oriented defence solutions.

Targeted type of applicants

Any eligible consortium as defined in Articles 10(4) and 9 of the EDF Regulation, which, in addition, is composed of SMEs, as defined in Commission Recommendation 2003/361/EC, and possibly of research organisations. Research organisations fulfilling the eligibility conditions of Article 9 of the EDF Regulation may join the consortium in the limit of 40% of the Union contribution to the action, but cannot be designated as coordinator. Non-SMEs fulfilling the eligibility conditions of Article 9 of the EDF Regulation may also participate to the action as subcontractors to the members of the consortium, in the limit of 30% of the total eligible costs of the action.

Budget

The Union is considering a contribution of up to EUR 17 500 000 to support proposals addressing any subject of interest for defence.

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

2.22.1. Topic EDF-2021-OPEN-R-SME: Research on innovative and future-oriented defence solutions

Specific challenge

This call encourages the driving role of SMEs in bringing forward innovation, agility and ability to progress technologies, possibly adapting them from civil to defence applications, in view of turning research results into products.

Scope

The proposals must address innovative defence technologies and solutions, including those that can 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.

Targeted activities

The proposals must cover one or more activities eligible for a research action, as referred in Article 10(3) of the EDF Regulation:

- activities that aim to create, underpin and improve knowledge, products and technologies, including disruptive technologies for defence, which can achieve significant effects in the area of defence;
- activities that aim to increase interoperability and resilience, including secured production and exchange of data, to master critical defence technologies, to strengthen the security of supply or to enable the effective exploitation of results for defence products and technologies;

- studies, such as feasibility studies to explore the feasibility of new or upgraded products, technologies, processes, services and solutions;
- the design of a defence product, tangible or intangible component or technology as well as the definition of the technical specifications on which such a design has been developed, including any partial tests for risk reduction in an industrial or representative environment.

However, the proposals cannot cover studies only.

Functional requirements

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

Expected impact

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

Funding information

The requested funding should match the ambition of the proposed action and be duly justified. In any case, the requested funding should not exceed EUR 4 000 000.

A lump sum approach will be used. For selected projects, the maximum EU contribution will be based on the eligible costs in the requested funding, but actual payments will be conditioned to the completion of work packages. Proposals should include clear descriptions of the proposed criteria to assess work package completion.

2.23. Call EDF-2021-OPEN-D: Open call dedicated to SMEs for development of innovative and future-oriented defence solutions

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

Proposals are invited against the following topic:

- **EDF-2021-OPEN-D-SME:** Development of innovative and future-oriented defence solutions.

Targeted type of applicants

Any eligible consortium as defined in Articles 10(4) and 9 of the EDF Regulation, which, in addition, is composed only of SMEs as defined in Commission Recommendation 2003/361/EC. Non-SMEs fulfilling the eligibility conditions of Article 9 of the EDF Regulation may participate to the action as subcontractors to the members of the consortium, in the limit of 30% of the total eligible costs of the action.

Budget

The Union is considering a contribution of up to EUR 36 000 000 to support proposals addressing any subject of interest for defence.

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

2.23.1. Topic EDF-2021-OPEN-D-SME: Development of innovative and future-oriented defence solutions

Specific challenge

This call encourages the driving role of SMEs in bringing forward innovation, agility and ability to adapt technologies from civil to defence applications and 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 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.

Targeted activities

The proposals must cover one or more activities eligible for a development action, as referred in Article 10(3) of the EDF Regulation:

- activities that aim to increase interoperability and resilience, including secured production and exchange of data, to master critical defence technologies, to strengthen the security of supply or to enable the effective exploitation of results for defence products and technologies;
- studies, such as feasibility studies to explore the feasibility of new or upgraded products, technologies, processes, services and solutions;

- the design of a defence product, tangible or intangible component or technology as well as the definition of the technical specifications on which such a design has been developed, including any partial tests for risk reduction in an industrial or representative environment;
- the system prototyping of a defence product, tangible or intangible component or technology;
- the testing of a defence product, tangible or intangible component or technology;
- the qualification of a defence product, tangible or intangible component or technology;
- the certification of a defence product, tangible or intangible component or technology;
- the development of technologies or assets increasing efficiency across the life cycle of defence products and technologies.

However, the proposals must cover at least one activity among the last six in the above list (*i.e.* design and beyond).

Functional requirements

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

Expected impact

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

Funding information

The requested funding should match the ambition of the proposed action and be duly justified. In any case, the requested funding should not exceed EUR 4 000 000.

A lump sum approach will be used. For selected projects, the maximum EU contribution will be based on the eligible costs in the requested funding, but actual payments will be conditioned to the completion of work packages. Proposals should include clear descriptions of the proposed criteria to assess work package completion.

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	Budget per call (up to in EUR)	Ceiling per proposal (up to in EUR)	Opening date[90]	Final date for submission [91]
EDF-2021-MCBRN-R	EDF-2021-MCBRN-R-CBRNDIM	18 500 000	18 500 000	09/09/2021	09/12/2021
EDF-2021-MCBRN-D	EDF-2021-MCBRN-D-MCM	50 000 000	50 000 000	09/09/2021	09/12/2021
EDF-2021-C4ISR-D	EDF-2021-C4ISR-D-HAPS	70 000 000	70 000 000	09/09/2021	09/12/2021
	EDF-2021-C4ISR-D-COMS				
EDF-2021-SENS-R	EDF-2021-SENS-R-IRD	38 000 000	38 000 000	09/09/2021	09/12/2021
	EDF-2021-SENS-R-RADAR				
EDF-2021-CYBER-R	EDF-2021-CYBER-R-CDAI	13 500 000	13 500 000	09/09/2021	09/12/2021
EDF-2021-CYBER-D	EDF-2021-CYBER-D-IECTE	20 000 000	20 000 000	09/09/2021	09/12/2021
EDF-2021-SPACE-D	EDF-2021-SPACE-D-SGNS	50 000 000	50 000 000	09/09/2021	09/12/2021
	EDF-2021-SPACE-D-EPW				
EDF-2021-DIGIT-R	EDF-2021-DIGIT-R-FL	18 500 000	18 500 000	09/09/2021	09/12/2021
EDF-2021-DIGIT-D	EDF-2021-DIGIT-D-MDOC	40 000 000	40 000 000	09/09/2021	09/12/2021
EDF-2021-ENERENV-D	EDF-2021-ENERENV-D-EEMC	133 000 000	133 000 000	09/09/2021	09/12/2021
	EDF-2021-ENERENV-D-NGES				
	EDF-2021-ENERENV-D-PES				
EDF-2021-MATCOMP-R	EDF-2021-MATCOMP-R-PHE	40 000 000	40 000 000	09/09/2021	09/12/2021
	EDF-2021-MATCOMP-R-RF				
EDF-2021-AIR-R	EDF-2021-AIR-R-NGRT	40 000 000	40 000 000	09/09/2021	09/12/2021
EDF-2021-AIR-D	EDF-2021-AIR-D-EPE	150 000 000	150 000 000	09/09/2021	09/12/2021
	EDF-2021-AIR-D-CAC				
EDF-2021-AIRDEF-D	EDF-2021-AIRDEF-D-EATMI	100 000 000	100 000 000	09/09/2021	09/12/2021
EDF-2021-GROUND-R	EDF-2021-GROUND-R-IW	10 000 000	10 000 000	09/09/2021	09/12/2021
EDF-2021-GROUND-D	EDF-2021-GROUND-D-FMGV	150 000 000	150 000 000	09/09/2021	09/12/2021
	EDF-2021-GROUND-D-UGVT				
	EDF-2021-GROUND-D-3CA				
EDF-2021-PROTMOB-D	EDF-2021-PROTMOB-D-SS	50 000 000	50 000 000	09/09/2021	09/12/2021
	EDF-2021-PROTMOB-D-DMM				
EDF-2021-NAVAL-R	EDF-2021-NAVAL-R-DSSDA	43 500 000	29 000 000	09/09/2021	09/12/2021
	EDF-2021-NAVAL-R-SSHM		14 500 000		
EDF-2021-NAVAL-D	EDF-2021-NAVAL-D-MMPC	60 000 000	60 000 000	09/09/2021	09/12/2021
EDF-2021-DIS-RDIS	EDF-2021-DIS-RDIS-QSENS	60 000 000	60 000 000	09/09/2021	09/12/2021
	EDF-2021-DIS-RDIS-NLOS				
	EDF-2021-DIS-RDIS-OTHR				
	EDF-2021-DIS-RDIS-AMD				
EDF-2021-OPEN-RDIS	EDF-2021-OPEN-RDIS-open	10 000 000	4 000 000	09/09/2021	09/12/2021
EDF-2021-OPEN-R	EDF-2021-OPEN-R-SME	17 500 000	4 000 000	09/09/2021	09/12/2021
EDF-2021-OPEN-D	EDF-2021-OPEN-D-SME	36 000 000	4 000 000	09/09/2021	09/12/2021

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

[91] 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 Tenders portal for update.

For the calls EDF-2021-DIS-RDIS, EDF-2021-OPEN-RDIS, EDF-2021-OPEN-R and EDF-2021-OPEN-D, resulting actions will be implemented through a 'lump sum' grant agreement (associated methodology and *Model Grant Agreement* will be published on the Funding & Tender portal after the opening of the calls). For all the other calls, the resulting actions will be implemented through 'actual cost' grant agreements (associated *Model Grant Agreement* will be published on the Funding & Tender portal after the opening of the calls). See Section 3.3.5 for additional information.

All calls for proposals are subject to a single-stage deadline model.

3.2. Evaluation procedure and conditions

The submitted proposals will be evaluated by the Commission according to Articles 150 and 200 of the Financial Regulation on the basis of the procedure and conditions described below.

3.2.1. Procedure

After the final submission deadline defined on the Funding & Tender portal, the European Commission evaluates the proposals on the basis of the criteria laid down in the EDF Regulation and further defined in the sections below. During the evaluation, the following assessment are performed:

a) **Admissibility**: determining if the received proposals meet the admissibility conditions (see Section 3.2.3). Proposals failing to meet admissibility conditions will be rejected, *i.e.* only proposals meeting the admissibility conditions will be subject to further assessment;

b) **Exclusion**: determining if all applicants and affiliated entities of an admissible proposals fall under exclusion grounds (see Section 3.2.4). Applicants and affiliated entities that are in an exclusion situation are excluded from participating in the call procedure and, as a consequence, from being awarded a grant;

c) **Eligibility**: assessing if the proposals meet all eligibility criteria (see Section 3.2.5), including:

   - eligibility of the proposed action;
   - eligibility of the entities involved in the action[92].

   Proposals which fail to meet any of the eligibility criteria will be rejected. Considering the principle of proportionality and the complexity of some criteria, the Commission will complete the eligibility assessment exclusively for proposals obtaining an evaluation score above the threshold;

d) **Ethics**: the ethics screening of all the proposals is a filtering step designed to identify the proposals that potentially pose complex ethical issues and that need to be further reviewed in the ethics assessment (see Section 3.2.6). The screening is done based on the Ethics Issues Table (Section 2 of the Part A sup of the *Submission form*) and the content of the proposal.

[92] Applicants, affiliated entities and subcontractors involved in the action.

e) **Selection**: assessing compliance of applicants and affiliated entities with the selection criteria (see Section 3.2.7), including:

   - financial capacity assessment;
   - operational capacity assessment.

   Proposals where applicants or affiliated entities fail to meet any of the selection criteria may be rejected.

f) **Award**: the Commission, assisted by independent experts, will assess the proposals against the award criteria, determining a score for each proposal answering the call (see Section 3.2.8).

   Eligible proposals in a given call for proposals scoring above the threshold (10.0/15.0) are sub sequentially ranked from the highest to the lowest score.

   The highest scoring proposals are subsequently proposed for funding by the Commission in the limit of the budget available for the call.

   Another set of proposals complying with all criteria but rejected by lack of budgetary appropriations can be placed on the reserve list. Proposals in the reserve list may be selected for grants if budgetary appropriation becomes available during the Grant Agreement Preparation phases.

In subsequent steps, all coordinators are informed about the results of the evaluation and coordinators of awarded consortia are invited 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.

During the grant agreement preparation, the Commission, assisted by external defence ethics experts, will also perform the ethics assessment for those proposals that pose complex ethics issues. For ethics issues not satisfactorily addressed in the proposal, further ethics requirements may be required. The results of the ethics assessments are considered in the grant agreement.

In addition, during the grant agreement preparation, the security framework for the selected proposals will be defined in accordance with Article 27(4) of the EDF Regulation (see Section 3.7).

3.2.2. Indicative timeline for evaluation and grant agreement signature

Indicative date for the information of the applicants on the outcome of the evaluation: six months from the final date for submission.

Indicative date for the signing of grant agreements: three months from the date successful applicants are informed.

3.2.3. Admissibility conditions

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

- applications must be submitted before the final date for submission;
- applications must be submitted electronically via the Funding & Tenders Portal electronic submission system (accessible via the topic page in the Search Funding & Tenders section). Paper, mail or e-mail submissions are NOT possible;
- applications must be submitted using the forms provided inside the electronic submission system once the calls are open. The structure and presentation must correspond to the instructions given in the forms;
- unless otherwise specified in the *Guide for applicants*, submission forms and supporting documents need to be provided as searchable pdf files;
- applicants must submit their proposal in one of the official languages of the Union (English language is encouraged);
- applications must be complete and contain all parts and mandatory Annexes [93] and supporting documents:
  - Part A of the *Submission form* needs to be filled in and submitted online directly on the Funding & Tender portal;
  - supplement to Part A ('Part A sup'), including its eight Annexes, and Part B of the *Submission form* need to be filled in offline and, once completed, submitted online, together with all requested supporting documents, on the Funding & Tender portal as a single password-protected (using AES-256 encryption method) zip archive with a size of less than 100 MB;
  - the password to access content of this single password-protected zip archive must be communicated before the final date for submission at the following email address: DEFIS-EDF-PROPOSALS-PWD@ec.europa.eu, indicating the proposal ID and the name of the corresponding zip archive. If this single password-protected zip archive itself contains other password-protected files, the associated passwords need to be communicated to the Commission before the final date for submission using the same email address[94], indicating the proposal ID and the name of the file(s) concerned;

  Applicants may usefully refer to the Guide for Applicants (available here) for more information.
- each proposal must only be submitted against one topic:
  - where a call is covering several topics (EDF-2021-C4ISR-D, EDF-2021-SENS-R, EDF-2021-SPACE-D, EDF-2021-ENERENV-D, EDF-2021-MATCOMP-R, EDF-2021-AIR-D, EDF-2021-GROUND-D, EDF-2021-PROTMOB-D, EDF-2021-NAVAL-R, EDF-2021-DIS-RDIS), proposals must only address one topic of this call;

[93] Annex 5 to the *Submission form* is not compulsory for the evaluation of submitted proposals and Annex 8 has to be filled in only by participants claiming the mid-cap status.
[94] Where necessary, separate emails for the different passwords may be sent by the originators concerned.

- proposals in response to the calls EDF-2021-OPEN-RDIS, EDF-2021-OPEN-R or EDF-2021-OPEN-D must address one clearly identified product, solution, material or technology which is of interest for defence.

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 (DEFIS-EDF-PROPOSALS@ec.europea.eu) well before the final date for submission of the call, in order to arrange the delivery of the classified part of their proposal.

Page limits

In addition to the above admissibility conditions, page limits will apply to parts of applications. The page limits, and sections subject to limits, will be clearly shown in the application templates in the Funding & Tenders Portal electronic submission system.

The limit for the Part B – Section 6 and 7 of the proposal is 60 pages for Research actions and 64 pages for Development actions. For Section 8, the limit for each work package is 2 pages.

If an application exceeds the limits, the pages after the limits for Part B – Section 6 and Section 7 and after each work package will be made invisible, and will not be taken into consideration by the Evaluation committee.

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.

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.

Each applicant and affiliated entities must declare on its honour that, at the time of the submission, it is 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 and affiliated entities (see Annex 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

The eligibility criteria fall mainly into two types, notwithstanding additional eligible conditions as set in this section:

a) eligibility criteria for the proposed action;

b) eligibility criteria for the entities involved in the action.

Assessment against these eligibility criteria will be performed based on all relevant information the applicants must provide at the time of the submission of their proposal.

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 relevant legal entity must inform the Commission, which will assess whether those eligibility criteria continue to be met and will address the potential impact of that change on the funding of the action.

3.2.5.1. Eligibility criteria for the proposed action

a) **A proposal will only be considered eligible if the proposed action complies with the general objectives of the fund (see Section 1), addresses the scope and covers the targeted activities described in the topic against which the proposal is submitted, as stated in Section 2 of this document**, hence addressing new defence products and technologies or the upgrade of existing ones.

b) Where addressing upgrade, the use of pre-existing information needed to carry out the action must not be subject to a restriction by a non-associated third country or a non-associated third-country entity directly, or indirectly through one or more intermediary legal entities, in such a way that the action cannot be carried out.

c) The action must only address one or more of the following activities:

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

Activities		Eligibility	
		Research action	**Development action**
(e)	The system prototyping of a defence product, tangible or intangible component or technology	No	Yes
(f)	The testing of a defence product, tangible or intangible component or technology	No	Yes
(g)	The qualification of a defence product, tangible or intangible component or technology	No	Yes
(h)	The certification of a defence product, tangible or intangible component or technology	No	Yes
(i)	The development of technologies or assets increasing efficiency across the life cycle of defence products and technologies	No	Yes

d) Unless specified otherwise in the calls addressing actions relating to disruptive technologies for defence or activities referred to under point (c) above:

- the action must be carried out by legal entities cooperating within a consortium of at least three eligible legal entities which are established in at least three different Member States or associated countries;
- at least three of those eligible legal entities established in at least two different Member States or associated countries must, during the entire period in which the action is carried out, not be controlled, directly or indirectly, by the same legal entity and must not control each other.

e) Actions for the development of products and technologies whose use, development or production is prohibited by applicable international law are not eligible for support from the Fund.

f) Actions for the development of lethal autonomous weapons without the possibility for meaningful human control over selection and engagement decisions when carrying out strikes against humans are not eligible for support from the Fund, without prejudice to the possibility of providing funding for actions for the development of early warning systems and countermeasures for defensive purposes.

g) The results of research actions and development actions supported by the Fund must not be subject to any control or restriction by a non-associated third country or by a non-associated third-country entity, directly, or indirectly through one or more intermediate legal entities, including in terms of technology transfer.

h) The consortium involved in the action must demonstrate that the costs of the action that are not covered by Union support are covered by other means of financing, such as by Member States' or associated countries' contributions or co-financing from legal entities.

In addition, in the case of a development action:

i) Actions addressing activities referred to in point (d) above must be based on harmonised defence capability requirements jointly agreed by at least two Member States or associated countries. If such actions address also activity (c) in the purpose to define such harmonised defence capability requirements, these latter must be submitted at the latest following the completion of the activity (c), provided that it is demonstrated at the time of the submission of the proposal that at least two Member States or associated countries intend to jointly agree on such harmonised defence capability requirements.

j) With regard to actions addressing activities referred to in points (e) to (h) above, the consortium must demonstrate by means of documents issued by national authorities that:

- at least two Member States or associated countries intend to procure the final product or use the technology in a coordinated manner, including through joint procurement where applicable;
- the activity is based on common technical specifications jointly agreed by the Member States or associated countries that are to co-finance the action or that intend to jointly procure the final product or to jointly use the technology.

If such actions address also activity (d) in the purpose to define such common technical specifications, these latter must be submitted at the latest following the completion of the activity (d), provided that it is demonstrated at the time of the submission of the proposal that at least two Member States or associated countries intend to jointly agree on such common technical specifications.

3.2.5.2. Eligibility criteria for the entities involved in the action

'Subcontractors involved in the action' mentioned hereafter refers to subcontractors with a direct contractual relationship to a recipient (*e.g.* consortium members) or to an affiliated entity, other subcontractors to which at least 10 % of the total eligible costs of the action is allocated, and subcontractors which may require access to classified information in order to carry out the action. Subcontractors involved in the action are not members of the consortium.

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

- the Member States of the European Union (EU), including their outermost regions, and the overseas countries and territories (OCTs)[95] linked to them;
- the members of the European Free Trade Association which are members of the European Economic Area (EEA), in accordance with the conditions laid down in the

[95] Aruba (Netherlands), Greenland (Denmark), New Caledonia (France), French Polynesia (France), Saint Pierre and Miquelon (France), French Southern and Antarctic Lands (France), Wallis and Futuna (France), Saint Barthélemy (France), Bonaire Sint Eustatius and Saba (Netherlands), Curaçao (Netherlands), Sint Maarten (Netherlands).

Agreement on the EEA (associated countries), unless these members have opted out of the EDF[96].

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

- By way of derogation from this condition, a legal entity established in the Union or in an associated country and controlled by a non-associated third country or a non-associated third-country entity will be eligible to be a recipient or subcontractor involved in the action only if guarantees approved by the Member State or the associated country in which it is established in accordance with its national procedures are made available to the Commission.
- Those guarantees may refer to the legal entity's executive management structure established in the Union or in an associated country. If considered to be appropriate by the Member State or associated country in which the legal entity is established, those guarantees may also refer to specific governmental rights in the control over the legal entity.
- Those guarantees must provide assurances that the involvement in the action of such a legal entity 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 (CFSP) pursuant to Title V of the TEU, or the objectives set out in Article 3 of the EDF Regulation, and are compliant with the provisions on ownership and intellectual property rights (Articles 20 and 23 of the EDF Regulation).
- Those guarantees must in particular substantiate that, for the purposes of the action, measures are in place to ensure that:
  - **Control** over the legal entity is not exercised in a manner that 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 knowhow needed for the purposes of the action, or that undermines its capabilities and standards necessary to carry out the action;
  - **Access** by a non-associated third country or by a non-associated third-country entity to sensitive information relating to the action is prevented and the employees or other persons involved in the action have national security clearance issued by a Member State or an associated country, where appropriate;
  - **Ownership** of the intellectual property arising from, and the results of, the action remain within the recipient during and after completion of the action, are not subject to control or restriction by a non-associated third country or by a non-associated third-country entity, and are neither exported outside the Union or outside associated

[96] Pursuant to the adoption of the Decision of the EEA Joint Committee No 228/2021 of 28 July 2021 amending Protocol 31 to the EEA Agreement, on cooperation in specific fields outside the four freedoms, the participation of associated countries to the European Defence Fund is limited to legal entities established in the Kingdom of Norway.

countries nor accessible from outside the Union or outside associated countries without the approval of the Member State or the associated country in which the legal entity is established and in accordance with the objectives set out in Article 3 of the EDF Regulation (see Section 1 of this document).

- If considered to be appropriate by the Member State or the associated country in which the legal entity is established, additional guarantees may be provided.

c) Where no competitive substitutes are readily available in the Union or in an associated country, recipients and subcontractors involved in an action may use their assets, infrastructure, facilities and resources located or held outside the territory of the Member States or of the associated countries provided that such use does not contravene the security and defence interests of the Union and its Member States, is consistent with the objectives set out in Article 3 and complies with Articles 20 and 23 of the EDF Regulation.

The costs related to those activities will not be eligible for support from the Fund.

d) When carrying out an eligible action, recipients and subcontractors involved in an action may also cooperate with legal entities established outside the territory of the Member States or of associated countries, or controlled by a non-associated third country or by a non-associated third-country entity, including by using the assets, infrastructure, facilities and resources of such legal entities, 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 set out in Article 3 and must comply with Articles 20 and 23.

There must be no unauthorised access by a non-associated third country or other non-associated 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 shall be avoided.

The costs related to those activities will not be eligible for support from the Fund.

3.2.5.2.1. Additional eligibility conditions in case access to Galileo PRS information is needed for carrying out an action and in particular for applicants applying for the topic EDF-2021-SPACE-D-SGNS

The scope of the topic EDF-2021-SPACE-D-SGNS - Space and ground-based NAVWAR surveillance, will require legal entities involved in the proposals to have access to the Galileo public regulated service (PRS). Given the potential relevance of PRS positioning, navigation and timing services, other calls may also require participants involved in the proposals to have access to PRS.

Access to PRS is regulated by Decision No 1104/2011/EU of the European Parliament and of the Council on the rules for access to the public regulated service provided by the global navigation satellite system established under the Galileo programme (“PRS Decision”).

Accordingly, legal entities in charge of PRS-related activities within the action shall be clearly identified and shall be in possession of the relevant authorisations to execute the activity. This entails in particular:

a) a legal entity in charge of PRS-related activities shall be authorised by the Security Accreditation Board (SAB, as per Article 38 of the Regulation EU 2021/696[97]) in the PRS category required to execute the contract;

b) a legal entity authorised by the SAB for PRS security module manufacturing (SM) shall, in addition:

   i. either be owned solely or through majority ownership by a Member State;

   ii. or have nationals of Member States holding a personnel security clearance granted by a Member State appointed in its Board of Directors and have delegated to these nationals the exclusive authority to take decisions related to the PRS;

c) in addition to the above conditions, a legal entity in charge of activities requiring access to PRS CRYPTO information, shall demonstrate that it may access such information.

The above-mentioned conditions in a), b) and c) are verified by the Competent PRS Authority designated by the Member State in the territory where the legal entity in charge of the PRS-related activity is established, in accordance with Decision No 1104/2011/EU of the European Parliament and of the Council of 25 October 2011 on the rules for access to the public regulated service provided by the global navigation satellite system established under the Galileo programme.

For this purpose, such legal entities shall provide a confirmation issued by the Competent PRS Authority designated by the Member State in the territory where the legal entity is established, that the relevant authorisations to execute the activity are in place.

3.2.5.2.2. Additional eligibility conditions for the call EDF-2021-OPEN-R

- The consortium applying for funding under the call EDF-2021-OPEN-R must be composed of small and medium-sized enterprises (SMEs) and, to some extent, of research organisations. In any case, the coordinator must be an SME. The share of the EU contribution allocated to research organisations within the consortium cannot exceed 40% of the total EU contribution to the proposed action.
- SMEs must be understood as defined in EU Recommendation 2003/361[98].

  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. This status will be validated by the Commission services based on this self-assessment and requested evidence.
- Research organisation must be understood as legal entities meeting the following two cumulative conditions:
  - they are established as non-profit organisations;

[97] REGULATION (EU) 2021/696 OF THE EUROPEAN PARLIAMENT AND OF THE COUNCIL of 28 April 2021 establishing the Union Space Programme and the European Union Agency for the Space Programme and repealing Regulations (EU) No 912/2010, (EU) No 1285/2013 and (EU) No 377/2014 and Decision No 541/2014/EU.
[98] 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.

- they carry out research or technological development as one of their main objectives.

This status will be validated by the Commission services based on a self-declaration on the Funding and Tenders portal and requested evidence.

Legal entities which are not SMEs nor research organisations can participate in the action (as subcontractors) but cannot be part of the consortium.

For each member of the consortium and each affiliated entity, subcontracting will be strictly limited to 30% of its eligible costs. Subcontracting costs above 30% will lead to the rejection of the proposal.

3.2.5.2.3. Additional conditions for the call EDF-2021-OPEN-D

- The consortium applying for funding under the call EDF-2021-OPEN-D must be composed of small and medium-sized enterprises (SMEs) only.
- SMEs must be understood as defined in EU Recommendation 2003/361[99].

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. This status will be validated by the Commission services based on this self-assessment and requested evidence.

Legal entities which are not SMEs can participate in the action (as subcontractors) but cannot be part of the consortium.

For each member of the consortium and each affiliated entity, subcontracting will be strictly limited to 30% of its eligible costs. Subcontracting costs above 30% will lead to the rejection of the proposal.

3.2.6. Ethics

Every proposal is subject to an ethics review and must be completed before the grant agreement can be signed. The review is based on the content of the proposal, with a particular focus on the ethics self-assessment provided by the applicants in Section 2 of the Part A sup of the *Submission form*.

Ethics self-assessment: Applicants must flag and address potential ethics issues in the Ethics Issues table in Section 2 of the Part A sup of the *Submission form*. All ethics issues flagged must be addressed in the ethics self-assessment section (Section 2 of the Part A sup of the *Submission form*) and make reference, if appropriate, to the relevant content of the proposal in Part B. When a successful proposal is turned into a grant agreement, the ethics self-assessment becomes part of the description of the action (Annex 1 to the *Grant Agreement*) and may therefore create obligations to the beneficiaries.

[99] 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.

The ethics assessment can lead to an ethics clearance, to a conditional ethics clearance or to a request for additional information. Proposals which are considered not to be ethically acceptable will be rejected.

3.2.7. Selection criteria

Selection criteria are intended to assess the applicant's ability to complete the proposed action. 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.

3.2.7.1. Financial capacity

The applicants and affiliated entities 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:

a) balance sheet and profit and loss account for the last two financial years for which the accounts were closed;

b) audit report produced by an approved external auditor certifying the above-mentioned accounts for applicants and affiliated entities 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 and affiliated entity 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 recipients 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 recipient or to generate an income.

Where the financial capacity of an applicant (including the coordinator) or affiliated entity is not considered satisfactory, the Commission may adopt measures to protect the financial interests of the Union, such as reduced pre-financing or request for pre-financing guarantees.

3.2.7.2. Operational capacity

The applicants and affiliated entities 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 Annex 7 to the *Submission form*).

3.2.8. Award criteria and scoring

Each proposal which complies with the admissibility, exclusion and eligibility conditions will be assessed and scored by the Commission (assisted by at least three independent experts) against (i) six award criteria for research actions[100] and against (ii) eight award criteria for development actions[101]. The award criteria and aspects to be considered are listed below. Associated specific items that will be looked are reflected in the *Submission form*.

Each proposal (for a research actions or for a development actions) will be assessed on the basis of the following six award criteria:

Criterion 1. Contribution to excellence or potential of disruption in the defence domain, in particular by showing that the expected results of the proposed action present significant advantages over existing defence products or technologies.

- Excellence of the overall concept and soundness of the proposed approach for the solution, including main ideas, technologies and methodology.
- Compliance of the proposal with the specific challenge, scope, targeted activities, functional requirements and expected impact of the topic as set out in the call for proposals.
- Extent to which the objective and expected outcome of the action differs from and represents an advantage at strategic, technological or defence operational level over existing defence products or technologies, or has a potential of disruption in the defence domain.

Criterion 2. Contribution to the innovation and technological development of the European defence industry, in particular by showing that the proposed action includes ground-breaking or novel concepts and approaches, new promising future technological improvements or the application of technologies or concepts previously not applied in defence sector, while avoiding unnecessary duplication.

- Extent to which the proposal demonstrates innovation potential and contains ground-breaking or novel concepts and approaches (*e.g.* new products, services or business and

[100] 'Research action' means an action consisting primarily of research activities, in particular applied research and where necessary fundamental research, with the aim of acquiring new knowledge and with an exclusive focus on defence applications (see Article 2(11) of the EDF Regulation).
[101] 'Development action' means an action consisting of defence-oriented activities primarily in the development phase, covering new defence products or technologies or the upgrading of existing ones, excluding the production or use of weapons (see Article 2(12) of the EDF Regulation).

organizational models), new promising technological improvements, or the application of technologies or concepts previously not applied in the defence sector.

- Integration of existing knowledge and previous or ongoing R&D activities in the defence and civil sectors when applicable, while avoiding unnecessary duplication.
- Extent to which the innovations or technologies developed under this proposal could spin-off to other defence applications and products.

Criterion 3. Contribution to the competitiveness of the European defence industry by showing that the proposed action is a demonstrably positive balance of cost-efficiency and effectiveness thus creating new market opportunities across the Union and beyond and accelerating the growth of companies throughout the Union.

- Foreseen competitive advantage of the product/technology/solution vis-a-vis existing or planned products/technologies/solutions across the Union and beyond, including consideration given to the balance between performance and cost-efficiency of the future solution.
- Potential to accelerate the growth of companies throughout the Union, based on an analysis of the Union's internal market and the global market place, indicating, to the extent possible, the size and the growth potential of the market it addresses as well as expected volumes of sales both within and outside of the Union.
- Strength of the IP strategy (*e.g.* patents) associated with the solution to support the competitiveness and growth of the company.

Criterion 4. Contribution to the autonomy of the EDTIB, including by increasing the non-dependency on non-Union sources and strengthening security of supply, and to the security and defence interests of the Union in line with the priorities referred to in Article 3.

- Extent to which the proposed action will contribute to the autonomy of the EDTIB by increasing the Union's industrial and technological non-dependency from third countries.
- Beneficial impact that the proposed activities will have on the strength of the European security of supply, including the creation of a new supply chain.
- Extent to which the project outcome will contribute to the defence capability priorities agreed by Member States within the framework of the Common Foreign and Security Policy (CFSP), and in particular in the context of the Capability Development Plan. Where appropriate, extent to which the proposal addresses regional or an international priorities when they serve the security and defence interests of the Union as determined under the CFSP, where they do not exclude the possibility of participation of any Member State or associated country.

Article 3 of the regulation establishing the European Defence Fund refers to 'defence capability priorities commonly agreed by Member States within the framework of the Common Foreign and Security Policy (CFSP) and in particular in the context of the CDP. In that regard, regional and international priorities, when they serve the security and defence

interests of the Union as determined under the CFSP, and taking into account the need to avoid unnecessary duplication, may also be taken into account, where appropriate, where they do not exclude the possibility of participation of any Member State or associated country.'

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://eda.europa.eu/publications-and-data/latest-publications/the-eu-capability-development-priorities.

Criterion 5. Contribution to the creation of new cross-border cooperation between legal entities established in Member States or associated countries, in particular SMEs[102] and mid-caps[103] with a substantial participation in the action, as recipients, subcontractors or as other legal entities in the supply chain, and which are established in Member States or associated countries other than those where the legal entities cooperating within a consortium which are not SMEs or mid-caps are established.

- Extent to which the proposed action will create new cross-border cooperation between legal entities established in Member States or associated countries, in particular SMEs and mid-caps, especially compared to former activities in the technological area of the call and taking into account the specificity of the market.
- Planned future cross-border cooperation between legal entities established in Member States or associated countries and cooperation opportunities created by the proposed activities.
- Extent to which SMEs and mid-caps which cooperate cross-border participate substantially and industrial or technological added value brought by them.

Criterion 6. The quality and efficiency of the carrying out the action.

- Effectiveness and practicality of the structure of the work plan (work breakdown structure) including the timing and inter-relations of the different work packages and their components (illustrated by a Gantt chart, Pert chart or similar).
- Usefulness and comprehensiveness of the milestones and deliverables of the project. Coherence and clarity of the criteria for reaching the milestones, which should be measurable, realistic and achievable within the proposed duration.
- Appropriateness of the management structures and procedures, including the decision-making mechanisms, to the complexity and scale of the project. Quality of the risk management, including identification and assessment of the project specific critical risks,

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

which could compromise the achievement of the stated project's objectives and detail of proposed risk treatments (*e.g.* mitigation measures).

- Appropriateness of the allocation of tasks and resources to consortium members, ensuring that all consortium members and associated partners have a valid and complementary role. Allocation of the work share that ensure a high level of effectiveness and efficiency for carrying out the action.

In addition to the six award criteria listed above, proposals for development actions will be assessed on the basis of the following additional two award criteria:

Criterion 7. The contribution to increasing efficiency across the life cycle of defence products and technologies, including cost-effectiveness and the potential for synergies in the procurement, maintenance and disposal processes.

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

Criterion 8. The contribution to the further integration of the European defence industry throughout the Union through the demonstration by the recipients that Member States have undertaken to jointly use, own or maintain the final product or technology in a coordinated way.

- Number of Member States that have committed to jointly use, own or maintain the final product or technology in a coordinated way, as demonstrated in the supporting documents.
- Contribution of the above-mentioned commitments by Member States to the integration of the European defence market throughout the Union and contribution of the proposal to the increase in cooperation potential between Member States.

Evaluation scores will be awarded for the criteria, not for the different aspects listed below each criterion. Each criterion will be scored out of 5, with half-points allowed, 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.

Depending on the type of actions, the following weightings will apply to the criteria:

	Weighting	
	Research actions	**Development action**
Criterion 1	x2	x2
Criterion 2	x2	x1
Criterion 3	x1	x1
Criterion 4	x1	x2
Criterion 5	x2	x2
Criterion 6	x1	x1
Criterion 7	*Not applicable*	x1
Criterion 8	*Not applicable*	x1

The score of a proposal will be determined by computing the weighted sum of the scores against each relevant award criterion and normalizing it to 15. The individual score of a proposal will therefore range from 0.0 to 15.0. It will be given with one significant digit following the decimal point (resolution of 0.1).

The final assessment and score of a proposal will result from a consensus of the Evaluation committee. The general threshold is set to 10.0 points out of 15 points. Proposals that will get a final consensus score below the threshold will be rejected.

3.2.9. 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 for proposals mentions that several actions may be funded, the next proposals on the ranking list may also be awarded subject to the availability of budget and provided that these proposals address different topics or different defence products, solutions, materials or technologies from those already awarded.

The following approach will be applied successively for every group of *ex aequo* proposals in order to determine a priority order for proposals with the same score, starting with the highest scored group, and continuing in descending order:

a) proposals that address topics not otherwise covered by more highly ranked proposals, will be considered to have the highest priority;

b) the proposals identified under (a), if any, will themselves be prioritised according to the scores they have been awarded for criterion 1 (Excellence or potential of disruption). When these scores are equal, priority will be based on scores for criterion 2 (Innovation and technological development). When these scores are equal, priority will be based on scores

for criterion 3 (Competitiveness). When these scores are equal, priority will be based on scores for criterion 5 (Creation of new cross-border cooperation);

c) if necessary, any further prioritisation will be based on the number of Member States or associated countries, in which applicants involved in the proposal are established;

d) the method described in (a), (b) and (c) will then be applied to the remaining ex aequos in the group.

The Commission will adopt an award decision based on the ranking list (main and reserve list) after having consulted the Member States through the EDF Programme Committee. Applicants of selected proposals will be invited 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 to enter into Grant Agreement Preparation (GAP).

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 (direct and indirect) provided and justified by the applicants at the time of submission of the proposal (see Annex 2 to the *Submission form*).

Indirect eligible costs must be determined by applying a flat rate of 25% of the total direct eligible costs of the action, excluding direct eligible costs of subcontracting and support to third parties and any unit costs or lump sums which include indirect costs.

As an alternative, indirect eligible costs may be determined in accordance with the recipient's usual cost accounting practices on the basis of actual indirect costs provided that those cost accounting practices are accepted by national authorities for comparable activities in the defence domain, in accordance with Article 185 of the Financial Regulation, and that they have been communicated to the Commission by the recipient.

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 (generating knowledge, integrating knowledge, studies, design, prototyping, testing…), applying the baseline funding rates, as described in Section 3.3.2, to the eligible costs of the activity concerned. For development actions, 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%.

The maximum Union financial contribution for a given activity, including the bonus, cannot exceed the values provided in Section 3.3.4.

For that purpose, the applicants must provide and justify eligible costs for each activity (see Annex 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 cover one type of activity only;
- 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 (or to the ceiling set for individual proposals where provided in the call text).

3.3.2. Applicable baseline funding rates

Activities		Baseline funding rate	
		Research action	**Development action**
(a)	Activities aiming to create, underpin and improve knowledge, products and technolog*ies,* including disruptive technologies, which can achieve significant effects in the area of defence	100% of eligible costs	*Not applicable*
(b)	Activities aiming to increase interoperability and resilience, including secured production and exchange of data, to master critical defence technologies, to strengthen the security of supply or to enable the effective exploitation of results for defence products and technologies	100% of eligible costs	Up to 65% of eligible costs
(c)	Studies, such as feasibility studies to explore the feasibility of new or improved technologies, products, processes, services and solutions	100% of eligible costs	Up to 90% of eligible costs
(d)	The design of a defence product, tangible or intangible component or technology as well as the definition of the technical specifications on which such design has been developed which may include partial tests for risk reduction in an industrial or representative environment	100% of eligible costs	Up to 65% of eligible costs
(e)	The development of a model of a defence product, tangible or intangible component or technology, which can demonstrate the element's performance in an operational environment (system prototype)	*Not applicable*	Up to 20% of eligible costs
(f)	The testing of product, tangible or intangible component or technology	*Not applicable*	Up to 45% of eligible costs
(g)	The qualification of tangible or intangible component or technology	*Not applicable*	Up to 70% of eligible costs
(h)	The certification of product, tangible or intangible component or technology	*Not applicable*	Up to 70% of eligible costs
(i)	The development of technologies or assets increasing efficiency across the life cycle of defence products and technologies	*Not applicable*	Up to 65% of eligible costs

3.3.3. Additional number of percentage points (bonus) to the baseline funding rate (for development actions only)

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 a project of the permanent structured cooperation (PESCO)	+ 10%
SME bonus	
Proportion of eligible costs allocated to SMEs established in the EU or associated countries ≥ 10% (for the activity concerned)	Proportion of eligible costs allocated to non-cross-border SMEs established in the EU or associated countries (up to maximum 5%) + Twice the proportion of eligible costs allocated to cross-border SMEs established in the EU or associated countries
Mid-cap bonus	
Proportion of eligible costs allocated to Mid-caps established in the EU or associated countries ≥ 15% (for the activity concerned)	+ 10%

'**SMEs**' means small and medium-sized enterprises as defined in the Annex to Commission Recommendation 2003/361/EC.

'**cross-border SMEs established in the EU or associated countries**' must be understood as SMEs established in Member States or associated countries other than those in which the member of the consortium that are not SMEs are established.

'**non-cross-border SMEs established in the EU or associated countries**' are SMEs established in the Member States or associated countries in which the member of 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 EU Recommendation 2003/361[104].

[104] 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.

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 Annex 1 to the *Submission form*.

3.3.4. Applicable maximum funding rates

Activities		Maximum funding rate[105]	
		Research action	**Development action**
(a)	Activities aiming to create, underpin and improve knowledge, products and technolog*ies,* including disruptive technologies, which can achieve significant effects in the area of defence	100% of eligible costs	*Not applicable*
(b)	Activities aiming to increase interoperability and resilience, including secured production and exchange of data, to master critical defence technologies, to strengthen the security of supply or to enable the effective exploitation of results for defence products and technologies	100% of eligible costs	Up to 100% of eligible costs
(c)	Studies, such as feasibility studies to explore the feasibility of new or improved technologies, products, processes, services and solutions	100% of eligible costs	Up to 100% of eligible costs
(d)	The design of a defence product, tangible or intangible component or technology as well as the definition of the technical specifications on which such design has been developed which may include partial tests for risk reduction in an industrial or representative environment	100% of eligible costs	Up to 100% of eligible costs
(e)	The development of a model of a defence product, tangible or intangible component or technology, which can demonstrate the element's performance in an operational environment (system prototype)	*Not applicable*	Up to 55% of eligible costs
(f)	The testing of product, tangible or intangible component or technology	*Not applicable*	Up to 80% of eligible costs
(g)	The qualification of tangible or intangible component or technology	*Not applicable*	Up to 80% of eligible costs
(h)	The certification of product, tangible or intangible component or technology	*Not applicable*	Up to 80% of eligible costs
(i)	The development of technologies or assets increasing efficiency across the life cycle of defence products and technologies	*Not applicable*	Up to 100% of eligible costs

[105] Baseline funding rates, plus the maximum possible cumulative bonuses.

3.3.5. Form of the grant

As a rule, the beneficiaries of an awarded grant will sign an actual cost grant agreement where a maximum grant amount is set in the agreement and the final grant will be liquidated at the end of the action on the basis of the actual costs of the action declared by the beneficiaries (final financial statement certified by an approved external auditor).

By derogation, for the calls EDF-2021-DIS-RDIS, EDF-2021-OPEN-RDIS, EDF-2021-OPEN-R and EDF-2021-OPEN-D, beneficiaries will sign a lump sum grant agreement where the amount of the grant will be fixed by the Commission on the basis of the estimated actual eligible costs at termination of the action as justified by the applicants in the application. The payment of the grant will then be made against the approval of the deliverables due in accordance with the grant agreement.

Please note that the provisions of the *Model Grant Agreements* that will be available on the Funding & Tender portal after the opening of the calls, will not be open for discussion or negotiation with the future recipients.

3.4. Duration of an action

The duration of the proposed action would generally not be expected to exceed four years. Any duration beyond this timeframe should be duly justified and substantiated, in Part B of the proposal, against the content and objectives of the proposed action.

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 as such 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 should also include arrangements regarding the intellectual property rights and regarding the security of the information relating to the carrying out of the action.

3.6. Grant agreement

For each proposal selected for award, the coordinator of the consortium will be invited to enter grant agreement preparation (GAP) with the Commission. *Model Grant Agreements*, subject to the form of the grant applicable to the call (actual costs or lump sum), will be available here after the opening of the calls.

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 recipients.

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

- where Member States have appointed a project manager, the Commission will consult the project manager on the progress made with regard to the action before the payment is executed;
- in addition to the deliverables identified by the applicants in their proposal, specific periodic reports and a final report will be requested from 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 Articles 28(1), 29(2) and 29(3) of the EDF Regulation. This will include, for instance, data on cross-border participation, including of SMEs and mid-caps, in actions carried out under the Fund, as well as the integration of SMEs and mid-caps in the global value chain, information on the countries of origin of the recipients, on the registration of patents and, where possible, the distribution of the generated intellectual property rights.

3.7. Actions involving the handling of classified information[106]

Pursuant to Article 27(4) of the EDF Regulation, the originatorship of classified foreground information generated in carrying out a research or development action must be decided upon by the Member States on whose territory the recipients are established.

To that end, 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 the necessary information for carrying out the research or development action.

If no such specific security framework is set up by those Member States, the Commission must set up the security framework for the action in accordance with the Decision (EU, Euratom) 2015/444[107].

The applicable security framework for the action shall in any event be put in place before the signature of the funding agreement or the contract.

[106] Restricted and above. Further details are provided in the Annex to this document.
[107] OJ L 72, 17.3.2015, p. 53–88.

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 DEFIS-EDF-proposals@ec.europa.eu. However, questions received after 1 December 2021 may not be answered by the Commission before the deadline for submission of the proposals. Any questions or replies will not constitute any ground to claim any expectation concerning the selection of the proposal or the award of the grant.

Annex on security aspects

This Annex spells out the main Security Aspects applicable to the EDF calls for proposals for 2021. It recalls the general requirements for the performance of the tasks identified in the calls, which may involve the handling of classified information.

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

1. Definitions

ACTION means, in the light of Regulation (EU) 2021/697 of the European Parliament and of the Council of 28 April 2021 establishing the European Defence Fund, the project selected under the Programme which the Consortium is to carry out.

RECIPIENT means a legal entity with which a funding or financing agreement has been signed or to which a funding or financing decision has been notified.

CLASSIFIED INFORMATION means information or material, in any form, the unauthorised disclosure of which could cause varying degrees of prejudice to the interests of the Union, or of one or more of the Member States, and which bears an EU classification marking (EUCI) or a corresponding classification marking, as established in the Agreement between the Member States of the European Union, meeting within the Council, regarding the protection of classified information exchanged in the interests of the European Union. 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 Annex.

CONSORTIUM means a collaborative grouping of applicants or recipients that is subject to an agreement and constituted for the purpose of carrying out an action under the Fund;

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.

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 means data, knowhow or information generated in the operation of the Fund, whatever its form or nature.

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 up to level granted.

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.

2. General conditions

Pursuant to Article 27(4) of the EDF Regulation, in case the implementation of the grant involves the handling of classified information, Member States on whose territory the recipients 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.

3. 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. 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.

5. Other provisions

Where a recipient 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 recipients 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 Annex - 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

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.