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

Budget

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

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

Objectives

The evolution of threats:

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

The operational context:

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

The technological context:

The overall protection of armoured vehicles keeps improving thanks to passive and active protection systems as well as additional layers of protection or new structure materials (lighter and more resistant). Future dismounted soldiers may benefit from mobility enhancement (with the use of light exoskeletons for instance), which will make them more agile. Automation may also play a key role in transforming future battlefields. Indeed, it may pave the way towards insensitive enemy lethal autonomous weapon systems and to fleets of UAV34s or ground robots, which would benefit from their numeric advantage to deal with traditional opponents. We can expect opponents that allow robotic attacks, unrestricted by man-in-the- loop for target engagements, forcing us to fight vehicle duels at machine speed. Moreover, long-range precision fires will keep developing, as well as electronic warfare capabilities. Finally, our forces may have to deal with classical ever-improving ammunitions as well as with CBRN35 and cyber-attacks or directed energy weapons.

Technical challenges:

- Integrate real time data from a variety of sources;

- Evaluate and process big data in constrained time;

- Elaborate a middleware architecture for a future secure network and battle management system allowing efficient data distribution as well as collaborative services between platforms from different countries possibly using heterogeneous hardware solutions36 also from different countries. The focus of this robust and secure network is on tactical level from brigade and lower since this is crucial for conducting land operations. In fact, multinational and national interoperability and data exchange is primarily lacking at the lowest levels (bottom-up approach to create a solution for the current capability gap). However, every nation requires joint interoperability and data exchange between all systems of systems at all levels. Moreover, the largest technical challenge can also be foreseen at the lower levels (company, platoon etc);

- Enhance interconnectivity and range of communication systems;

- Enhance interoperability between platforms, at platform (legacy and new) and dismounted soldier level;

- Ensure cyber security and active defence of the networks;

- Ensure maintainability and technical relevance of software-based systems;

- Ensure interoperability over different generations of digital systems;

- Ensure the integration of different Battlefield Combat Identification systems;

- Elaborate C2-system architectures to avoid information overload, adapting information push to different user groups, whilst ensuring mutual situational awareness across the network;

- Ensure Electronic Warfare (EW) security, e.g., by enhancing the ability to quickly adapt to EW-threats by automated switching between different communication platforms, in addition to the existing frequency jumps in current radios;

- Ensure provisions for trend analysis enabled by algorithms in order to predict possible future adversaries' activities;

- Exploit space-based technologies, ensuring the full availability of space services;

- Develop data fusion functionality with possibility to use AI technology;

- Ensure compatibility and interoperability with Combat Cloud Services. A joint approach should be pursued from the beginning of the process. In fact, for some operations, with the development of EU collaborative warfare capabilities (ECOWAR) in the other subgroups (air, maritime, multi-domain), it is foreseeable that collaborative warfare will develop some joint capabilities for specific use-cases and interoperability with joint Strategic Command and Control Systems.

Scope and types of activities

Scope

The proposals must address the development of innovative multi-national collaborative land

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

They must include:

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

- Identification of key enabling technologies;

- Definition of a coordinated approach concerning middleware architecture frameworks for land collaborative combat;

- Analysis of applicable standards and norms as well as evolution proposals;

- Definition and realization of incremental real world key demonstrations (including preliminary prototyping within simulated environment).

Expected advantages and benefits of collaborative warfare:

- Speed up and improve the decision-making process;

- Reduce the time between threat detection / aggression and action or respond (e.g., manoeuvre, fire, close air support);

- Make critical information available at the right time to the right user ("actionable intelligence");

- Share knowledge / understand a situation, in real time or near real time with our neighbouring units;

- Create and share a recognized ground picture (RGP) in real time (condition of NATO Federated Mission Network (FMN) spiral 2 and higher), to constantly update situational awareness and feed the Joint Common Operational Picture (JCOP) and vice versa;

- Enable friendly forces to gain the tactical initiative (which means presenting the situation and the options in an adequate way to the operator using adapted human machine interface (HMI), for instance with augmented reality, modelling or simulation);

- Enable a dynamic and reliable interoperability when using the different manned/unmanned platforms (size, weight, type, theatre crossing speed, presence of unmanned systems etc.) and therefore trigger mobility skills to define a complex combat collaboration among systems, which can capitalize information in order to interact efficiently and proficiently.

Consequently:

- Enhance the use of different land assets through the effective use of battle space management;

- Increase the situational awareness at the tactical level (brigade and lower);

- Reduce risks of friendly fires and collateral damage, mitigate other potential operational risks;

- Improve interoperability (in particular with respect to NATO standards including FMN compliancy, providing a further development for the European Defence Forces interoperability level);

- Ensure provisions for future "sensor to shooter" functionality;

- Increase agility and flexibility in C2 structure;

- Enhance tactical performance and decision making;

- Enhance the effectiveness and the efficiency of the military action.

Types of activities

The following types of activities are eligible for this topic:

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

Functional requirements

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

Information sharing in order to build collective capabilities (and extend national resources while

keeping full control on them):

- Map sharing: to benefit from a common and possibly extended digitized representation of the ground (with the same geographic characteristics: same typology, same grid references, etc.) seems to be a necessity for data exploitation and will facilitate a common understanding of tactical situations

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

- Collaborative blue force tracking: geolocalisation can extend to multiple friendly platforms with aggregations to present the localization of units of different sizes;

- Sharing information related to the target and disseminate the battle damage assessment;

- Collaborative observation / intelligence, surveillance and reconnaissance (ISR) (sharing of e.g., pictures, videos, plots) at the tactical level (brigade and lower);

- Sharing enemy observations, including detection, recognition, identification, location and tracking;

- Mobility information (for instance to allow coordination of manoeuvres);

- Information concerning specialized support chains (combat engineering, resupply, logistics, maintenance etc);

- Exchange of combat status of own and neighbouring units (such as operative readiness, energy, etc);

- Information allowing hybrid applications with civil or other partners (e.g., police).

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

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

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

- Enhanced collaborative blue force tracking: geolocalisation can be refined through data fusion (for instance through triangulation between multiple observations or sensors);

- Collaborative detection – reconnaissance – identification – localization and tracking: refine enemy force understanding through data fusion;

- Collaborative environment modelling: refine and extend environment models through data fusion. This function could also include coordination to map the environment (observation can also apply more broadly to quickly explore a larger area with different platforms from several countries) or to define the best observation sectors for battlefield surveillance, potentially using remote sensors such as UAVs;

- Collaborative scene analysis (including for instance change analysis or detection of abnormal events);

- Enemy tactical picture: to be refined through automated data fusion;

- Tactical situation sharing (such as RGP);

- Command and control (C2) coordination tools: C2 can be coordinated to achieve collaborative manoeuvres within the coalition and if it is associated to artificial intelligence (AI) to help plan itineraries and analyse the situation.

Technical solutions should be based on:

- Flexible middleware architectures for various levels of integration of multinational forces within combined network-enabled operations allowing an efficient (e.g., seamless, flexible, cyber protected) communication network combined with a unified battle management system to be progressively integrated into a framework of secured combat cloud as a key game changer37;

- Scalable architecture to adapt to the several missions and working levels;

- The middleware should allow to control the electromagnetic and data signature of the unit;

- Standard interfaces to guarantee the interoperability with the existing and new platforms. A robust and open on-board platform network;

- Automated data fusion (e.g., image processing, sensor fusion, multi-criteria optimization, meta data management, simultaneous multi sensor usage) and HMI;

- Modern and innovative HMI able to integrate data coming from:

    - Various kinds of sensors (e.g., optronics, warning systems, navigation sensors);
    - Various kinds of effectors.

Standards and norms:

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

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

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

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

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

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

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

- Integrate the most mature functions into target systems (e.g., vehicles or UxV associated with specific battlefield management systems and radios), which would be defined by the pMS;

- pursue the maturation of prospective functions;

- study new functions dedicated to new use cases for common collaborative action beyond information sharing and observation (e.g., collaborative fires or collaborative protection).

Expected impact

- Enable secured network-enabled operations relying on the distribution of basic warfighting functions (e.g., observation leading to ISR, command & control, fire management, protection) among different combat systems;

- Rebuild a credible deterrent in terms of land combat capability, by introducing in shortest possible time advanced solutions for collaborative combat within coalitions;

- Introduce new innovative collaborative combat technologies and capabilities that can be adapted to various manned or unmanned platforms;

- Provide a governmental EU agreed framework that industry can use to build state of the art and highly innovative systems dedicated to collaborative/federated land combat for emerging and future capability needs;

- Provide solutions that solve emerging/future capability needs of several Member States and Norway with maximum commonality and modularity;

- Increase strategic autonomy of EU concerning technologies and products.