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 main functional requirements.

Up to one action may be funded under this call.

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 & 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 & 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 & 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 between of solutions & 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.