CYBER, C4ISR

(SE) Robust Communication Infrastructure and Networks (ROCOMIN)

(Established in March 2023)

For Public Release

PROJECT DESCRIPTION

The development in the area of robust communication infrastructure and network as a basis for C2 systems, is in a paradigm shift. The use of civilian technology in military applications is becoming more important at the same time as the pace of development is increasing. Networks are in fast digitalisation within the armed forces and secure interoperability will be key to future battlefield dominance at all levels.

New development principles are being based on the so called DevSecOps – development, security, and operations - a continuous development integrating security in every phase of the software development lifecycle, which is key for future development in the military domain. This new way of working needs a coordinated approach and methods that ROCOMIN plan to introduce. ROCOMIN aims to identify needs and harmonise requirements and other activities affected by or related to the area of robust communications infrastructure.

The areas for cooperation are:

Research and development:

To define and influence roadmaps as well as support and manage results from multilateral cooperation in the frame of PESCO, PADR, EDIDP, EDF and EDA projects. The focus here will be to enhance synergies between projects and to address technology gaps.

Capability management:

- To harmonise requirements (operational, technical), analyse user processes, develop CONOPS, and scenarios (using cases) to support development.
- To harmonise regulations and security aspects.
- To ensure conformity to NATO activities, especially in the frame of the Federated Mission Networking (FMN) initiative.

Studies, analysis, reports (note, this is a non-exhaustive list):

- To examine modern antenna technology in order to improve Satcom on-the-move from e.g., land-based platforms – especially in northern latitudes. A particular interest is how to integrate antennas in the hull of platforms.
- To examine how to extend the backhaul link from a mobile tactical network using low-cost UAV and new antenna technology. Specifically examine how commercial technology, like 5G, can reduce overall cost and add value to solutions.
- To examine distributed computing power in a tactical network environment for enhanced situational awareness.
- To investigate vulnerabilities and their mitigation in order to achieve increased robustness and resiliency. Also, to investigate the benefits and possibilities of integration with existing tactical datalinks (TDL) networks.

SE, EE, FR, DE

BG, EL, IT, NL, PT

IDEATION
INCUBATION
EXECUTION
CLOSING

Contribution to the more binding commitments
Yes

Capability Perspective

CDP priority
Ground Combat Capabilities
Land Based Precision Engagement
Future Soldier Systems
Underwater and Seabed Warfare
Space Operations

CARD references
Soldier systems
C4ISTAR and Tactical CIS

Operational Viewpoint

HICG
CIS
Joint C2
C3
FMN

EDA support

No

OBJECTIVES/PRODUCTS

The objective is to catalyse studies, initiatives and demonstrators in selected ongoing projects within EDA/EDF/PESCO in order to increase EU capabilities through identifying, initiating and facilitating activities in the area of robust communication infrastructure and networks enabling military operations.

The desired outcome is a model for an AI driven management tool/instrument/architecture to program and adapt communication and networks infrastructure, equipment using the characteristics, standards and environment in order to ensure timely, safe and secure communications.

INDICATORS

Project Execution Year (PEY) and Project Completion Year (PCY):

DELIVERABLES ACHIEVED

Definition Military Robust Communication:

- Robust communication refers to communication infrastructure and networks that can resist to environmental and weather adverse conditions, resilient to congested and interfered electromagnetic environment, withstanding intentional and unintentional, external or internal disturbance (such as technical faults, natural disasters, signal disturbances or cyber threats), within peace, conflict or war contexts, guaranteeing timely, safe and secure interoperability among the member states' defence forces and compliance to military standards.

Common Requirements ROCOMIN:

- Communication and networks:
    - shall resist to environmental and weather adverse conditions.
    - shall be resilient to congested and interfered electromagnetic environment.
    - shall withstand intentional and unintentional, external or internal disturbance.
    - shall be guaranteeing timely, safe and secure interoperability among the member states' defence forces and shall be compliant with military standards.
        - Communication and networks should comply with Federated Mission Networking and Protected Core Network architectures defined by NATO for coalition networks.
        - should make sure to get leverage from dual use of latest civilian EDT in military applications.
- These common requirements should be addressed for all present and future CIS/ICT and Cyber-related projects, both in civil and military cooperation and operations. Enabling necessary legal frameworks should be adapted according to the specified needs.

CRITERIA FOR SUCCESS

ROCOMIN will achieve its objectives ensuring:

- interoperability and an increased connectivity among all-level military entities by using robust communication thus enabling Multi Domain Operations.
- cooperation of related projects and PoC's to get the insights of those projects' deliverables.
- sharing of its purpose and intent within the EU community.