EDF-2022-DA-CYBER-CIWT: Cyber and information warfare toolbox

Budget:

The Union is considering a contribution of up to EUR 33 000 000 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

General objective

The continuously and rapidly increasing flow of information in the information environment, facilitated through cyber capabilities, is a well-established fact. We are witnessing an increasing number of malicious actions targeting the information environment. In the more and more digitalized battlespace, the Cyber and Information domains become decisive to anticipate and manage conflicts in the full spectrum of threat activities from sub-threshold interference to open warfare.

Specific objective

Threats posed by new and evolving cyber and hybrid tools (e.g., disinformation, deep fakes) are fully part of Cyber and Information Warfare[24]. These threats need to be addressed with appropriate holistic resilience measures including detection and appropriate countermeasures. Cyber and Information Warfare system performance, in terms of total defence effectiveness and cooperation in cyber defence as referred in the EU Capability Development Plan Priorities, could be improved.

Scope and types of activities

Scope

Proposals are expected to address development of a European coherent library of software configurable components to easily integrate in Cyber and Information Warfare systems. This requires capabilities in detection, analysis, fusion and threat targeting to support activities of Cyber and Operational Centres for operational use cases (e.g., attacks against deployed forces in operations; attacks aiming to destabilize one and/or several European countries). Various relevant technologies processing multi-sources data for Cyber and Information Warfare operations needs to be addressed. In addition, enabling items such as standardization, data exchanges rules, multi-source fusion applications, AI-based analytics, methods & tools for integration, qualification in defence systems should be covered. The disinformation phenomenon includes also cultural and social aspects (so called “social science & humanity”) that may be studied by multidisciplinary teams to provide a holistic perspective.

The outcome is expected to become both a reference repository of AI-based configurable applications and an experimental platform for the various AI techniques addressing the specificities of Cyber and Information Warfare (for example disinformation tracking applications).

[24] https://www.nato.int/nato_static_fl2014/assets/pdf/2020/5/pdf/2005-deepportal4-information-warfare.pdf

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 (optional
(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)

The proposals must include design and prototype activities. The proposal may include studies, testing, qualification, certification, and increasing efficiency activities.

The following tasks must be performed as part of the required activities:

(1) Define toolbox concept that enables the use/implementation of hardened AI techniques including rules, method and tools to develop, integrate, realize orchestration and share configurable assets (data, modules, analytics, applications, etc.) for Cyber and Information Warfare system;

(2) Provide standardization and interoperability recommendation;

(3) Functional analysis of typical scenarios covering use cases that will be implemented to support Toolbox demonstrations, such as:

- Attacks against deployed forces in operations;
- Attacks of hybrid nature below the threshold of conventional warfare against critical

entities and functions in whole-of-society, including defence and military.

(4) Operational concept of usage, including use of AI and efficient situation awareness tools, consistency with rules of engagement (RoE), management of counterintelligence, and trustworthiness;

(5) Algorithm prototyping, implementation and verification, including the data sets and metrics to be used to do so for the purpose of the above use cases;

(6) Development tools including algorithm insertion, integration in demonstration environment and run of demonstration to illustrate the use of the Toolbox for the two above use cases.

The proposals must substantiate synergies and complementarity with general command and control processes and functions, avoiding unnecessary duplication with projects previously awarded.

The following task may be performed as part of the activities:

- Studies regarding societal and cultural impact of disinformation and (blue &red) state- led communication campaigns.

The proposals could benefit from framework, or results coming from projects previously awarded, increasing synergies and effectiveness of targeted activities.

Functional requirements

Proposals should meet the following functional requirements:

I Information Warfare

Developing information manipulation identification, “Disinformation Tracking” use case (including modelling influence and opinion propagation, user behaviour analysis, community detection in social graphs, detect disinformation campaigns, identify disinformation, with trustworthiness score) in favour or against Information Warfare Operations in the context of Multidomain Operations.

In order to offer situational awareness and support to decision process, proposals should elaborate on:

- identified threats activities (hostile influencing avatars and groups);
- campaign with scorings levels like trust, importance (followers, retweets), severity and friendly targets;
- used artifacts (pictures, texts, video) that can be identified as fake/reused items;
- when possible, additional information providing hints on physical sources of information operations attacks (e.g., images metadata or details, IP addresses, etc.)
- identification of "archetypes or patterns” of fakes to increase interception capabilities, both in a ‘humanity’ and through a ‘technology’ approach;
- Interactions with other sources of information, such as open source and human intelligence (OSINT, HUMINT), that could be related with operations in cyber domain and used for optimisation and synchronisation.

II Emerging Technologies

Proposals should identify emerging technologies that can be applied on automatic image/video/text entities extraction/indexing/classification/fusion and be subject to further research and development, such as:

- Active Learning (to allow operators to make their own classifiers with their own data)
- Case-based Reasoning (CBR) or other metacognition enablers to create different levels of knowledge abstraction
- Transfer/Frugal Learning (to be able to learn from small amounts of data)
- Hard and Soft Fusion (to fuse data and information from different sensors and sources, including semantic information)
- Explainable AI (to ensure that all AI algorithms are transparent and that the operators can have a look into AI decisions for understanding if needed)
- High precision 3D modelling
- Method and toolkit for assessing performances and security aspects (ethics guidelines, elimination of biases, compliance with GDPR, system protection etc.).
- Situational awareness and corresponding decision aids (to track incidents, link them into a campaign, and issue recommendations and alerts).

III Standards and interoperability

To develop and promote assets in the Toolbox, proposals should comply requirements such as technology standards (API, encapsulation), data exchange and interoperability standards, intellectual property protection, traceability, and authentication.

Proposals should:

- Define a set of standards' proposals that allows multi-national collaboration, sharing of data and sharing of assets like for example machine-learning models for military use.
- Define guidance for AI-based defence projects development.
- Contribute to a proposal to standards integration of new technologies such as AI in Cyber and Information Warfare system and more broadly for defence application.
- Compile existing standards and contribute to a proposal to standards for trustworthy AI in defence.
- Ensure that the project leverages technological capabilities while at the same time addressing the ethical issues involved.
- Explore harmonisation of existing tactics, technologies, and policies.

<u>Expected impact</u>

The outcome is expected to contribute to:

- Optimizing the development and integration of analytics in Cyber and Information Warfare systems with the possibility to decrease cost;

- Increasing the European technological sovereignty in the field of Cyber and Information Warfare applications based on AI;
- Increasing of the overall Cyber and Information Warfare system performance as new technologies will give better results in terms of total defence effectiveness;
- Gain on costs, availability and interoperability by optimizing the development and integration of analytics in Cyber and Information Warfare systems and capitalizing at European level Cyber and Information Warfare assets.