EDF-2022-DA-CYBER-CSIR: Cybersecurity and systems for improved resilience

Budget

The Union is considering a contribution of up to EUR 27 000 000 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 for this topic

Objectives

General objective

Kinetic and digital military operations increasingly rely on computers and networked communications for information gathering, intelligence, coordination and weapon control. At the same time as the dependencies on digital technologies rapidly grows, so does the potential threats and vulnerabilities. The global community, military, and battlefield may be affected by increasing threats. Furthermore, the Internet of Things (IoT) has become widely integrated into a variety of sectors and industries, offering "readymade" solutions for surveillance, monitoring, healthcare, and military platforms. Examples for IoT devices are drones, software defined radios, sensors (cameras, humidity, temperature), TV devices, cars/vehicles). Many IoT solutions are designed primarily for functionality, without being properly secured. As a result, attacks on IoT environments have gained momentum due to the increased attack surface. Therefore, the need for cybersecurity services, including ensuring an appropriate level of control and prevention (e.g., over data, communications, systems), must be addressed.

Specific objective

Currently, many cybersecurity solutions are being used or under development or research. However, cyber threats continue to evolve affecting the systems and services on which today's community relies.

A test environment is imperative to determine how to enhance the security of a system, product, or component, through the generation of effective tests for analysing the system in question, its threat response capability, resulting in forensic dissemination, procedures, and proposals of improved architectures.

Most legacy specialized military systems are not directly vulnerable to cyber-attacks and malware employed in the open Internet, yet a growing use of ICT/IoT Commercial Off The Shelf (COTS) components and increasing connectivity may increment the likelihood of targeted attacks using the methods, if not the tools, used in cyber-attacks on the open Internet.

The increasing use of the cyber domain will require defence forces to operate in unexpected scenarios and consequently systems to function outside the environments they were designed for.

It is thus essential to understand the extent of the threat, develop infrastructure to continuously assess security against an evolving threat landscape, build resilience by guaranteeing mission assurance even with a partial compromise also using trustworthy hardware, software applications, communication protocols and trustworthy operating system.

Scope and types of activities

Scope

Proposals are expected to prepare, design and/or demonstrate a Cyber Physical Test lab with hardware and software tools supporting expertise focusing on generation of effective tests for common and relevant Cyber Physical systems, products and components with realistic data from a relevant use case.

It must provide capabilities for cybersecurity analysis of the actual and planned system architecture, including a demonstrated threat analysis of a selected system or component. Based on this analysis, the architecture can be updated in order to increase the security of the system to an appropriate level.

Integrated tools for automated cost-efficient cyber validation tests based on requirements indicated by international standards may be included. The tools should be able to emulate system being tested, store detailed configurations, conduct automated testing and validation of military architecture, store the results and be able to repeat testing periodically in a cost- effective manner, considering system reconfiguration and extension during the lifecycle and the updated threat landscape.

The proposals are expected to contribute to enhancing cybersecurity in the Member States and Norway critical digital information infrastructure- solutions and services within security, encryption and communication systems, from strategic to tactical level.

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 (optiona
(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 (optional)
(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 study and design activities. The proposal may include other eligible downstream activities.

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

- Phase 1: Perform requirements analysis, development of concepts and procedures, definition of architecture and design a Cyber Physical Test lab with expert hardware and software test tools and integrated tools for validation.
- Phase 2: Implementation and demonstration of a Cyber Physical Test lab with HW[25] & SW[26] test tools that focus on generation of effective test, forensic dissemination, procedures and architecture to ensure cybersecurity for common and relevant Cyber Physical systems, products and components, including addressing Digital Twin applications in the military supply chain over the lifecycle.

The final product/ system must be able to analyse the security of a system in order to ensure:

- Data integrity
- Data control
- Data Loss Prevention
- Communications control
- Meta Data control
- Operational control of Cyber Physical components for common and relevant Cyber Physical systems, products and components
- Ability to guarantee mission-essential capabilities even with partial compromise.

The final product (Cyber Physical Test Lab) must comply with existing and foreseen standards, including military standards.

[25] Hardware

[26] Software

Functional requirements

The proposal should support the development of the final product.

The final product (Cyber Physical Test Lab) should meet the following functional requirements:

- Provide physical access to dedicated computers for instrumentation and software development. Part of the Lab may be restricted (classified) according to specific needs deriving from the products and components being testedGenerate effective penetration tests to evaluate the security of a system or a component, using state-of-the art tools;
- Generate customizable network traffic for testing and evaluating systems and solutions, and their security;
- Provide specialized resources for simulating attacks with and extendable and customizable database cyber tools for network traffic, services, IoT devices and communication in a customizable with the capability to automate attacks;
- Provide solutions and support to develop and debug embedded systems;
- Perform static analysis of embedded software, in order to improve security in IoT;
- Configure Cyber Physical systems according to appropriate and robust architecture for specific and customised use by Member States and Norway;
- Address the use of Digital Twin applications in the military supply chain over the system lifecycle;
- Monitor and control the communications between cyber physical components, systems, and the external environment through a state-of-the-art software;
- Provide a library of procedures to render a component or a system safe to use under specific conditions;
- Create a database with information on the risk of using various components of a system;
- Provide recommendations on risk mitigating techniques and risk management for a system or a component of a system;
- Provide capability in order to store the configuration of systems/components to be tested, enabling efficient periodic testing and whenever possible automated setup of configuration to be tested;
- Provide capability to store results, formal description of the system being tested, performed attacks, attack propagation, effect on functionalities and services, and compute a set of KPIs specialized for different types of technology / solution being tested;
- The lab should be a centralized or federated system. Federation should be used when needed in order to ease testing and validation, within a common technical and methodological framework, of components of national interest;

Expected impact

The outcome should have a major impact on the Member States and Norway' economy and cybersecurity cooperation, through:

- Establishing state-of-the-art test facility and competences, procedures and forensic software for Cyber Critical systems.
- Enabling IoT third parties to be used in a more secure, effective and economical way both in legacy, and novel systems.
- Decreasing implementation cost and shortening implementation time for advanced cyber security systems for the cooperating Member States and associated countries.
- Enabling the use of secure third-party components in Cyber Critical systems, leading to increased flexibility and competitiveness for the cooperating Member States and associated countries.
- Contributing to the certification of systems and to the EU Cybersecurity Certification framework, including contributing to enhance "security by design" of new systems and identify threats related to the supply chain.