EDF Call Topic Proposal

This form shall be used to propose or elaborate a call topic for the EDF. Filled in forms should be addressed to DEFIS-EDF@ec.europa.eu.

Short description

The information below should be suitable for inclusion in a work programme.

Title

Next-Generation Cooperative Cyber Range Capability (NGENCR)

Category of actions 4. Cyber (Common and/or interoperable tools for cyber operations). Proposal for MAP and EDF Work Programme 2024.

Indicative EDF funding budget

48 M€

Targeted type of actions

☐ Research ☒ Development

Targeted types of activities

Studies – Such as feasibility studies to explore the feasibility of new or upgraded products, technologies, processes, services and solution. Design – The design of a defence product, tangible or intangible component or technology as well as the definition of the technical specifications on which such a design has been developed, including any partial tests for risk reduction in an industrial or representative environment. Prototyping – The system prototyping of a defence product, tangible or intangible component or technology. Testing – The testing of a defence product, tangible or intangible component or technology. Qualification – The qualification of a defence product, tangible or intangible component or technology. Certification – The certification of a defence product, tangible or intangible component or technology.

Short textual description

Year in MAP: 2024

Cyber range technologies have seen notable uptake over the last decade and they are now considered as a key cornerstone of any cyber defence and cyber security training and testing programme. These developments have been complemented by significant R&D investments both from national and international funding programmes such as the European Defence Fund (e.g., EDF-2021-CYBER-D-IECTE) and Horizon Europe (e.g., DIGITAL-ECCC-2022-CYBER-03-CYBER-RESILIENCE) with further support from strategic cooperation such as through PESCO Cyber Ranges Federation.

Technological investments and developments have mostly focused on various fundamental needs such as visualization, scoring, realistic scenarios, federation and so forth that in principle implement technological capabilities already existing in other cyber and IT solutions. Such developments have not necessarily been breakthroughs in the larger frame of technology but rather importing concepts and technologies already in use elsewhere but now tailored to the context of cyber ranges.

The objective of the current topic is to take further the ongoing cyber range technology roadmap by designing and implementing next-generation solutions. A key consideration must be on the cooperative approach in developing and using those cyber range technologies, thereby facilitating joint capability development.

Member State and associated country support

This section documents support from Member States and associated countries, possibly including potential co-financing, intention to procure the final product or use the technology in a coordinated way, etc.

Project is supported in total by 12 member-states. More particularly, they are enlisted as below.

Contact points

The table below gathers the contact information (including email addresses and phone numbers as deemed appropriate) of representatives interested in participating in the topic harmonisation.

AT	Florentin Schlager (florentin.schlager@bmlv.gv.at)
BE	Manfred Delaere (Manfred.delaere@pandora.be)
BG	
CY	
CZ	
DE	
DK	Nanna Kirstine Sondergaard Holt (FMI-SD-IAR14@mil.dk)
EE	Ander Allas (ander.allas@kaitseministeerium.ee)
EL	Dimitrios Filiagkos (dfiliagkos@gdaee.mil.gr)
ES	
FI	Anna Oksanen (anna.oksanen@gov.fi) ; Niklas Backlund niklas.backlund@gov.fi
FR	
HR	
HU	
IA	
IT	
LT	
LU	Aziliz Guerin (Aziliz.Guerin@mae.etat.lu) ; Christian Hutter (Christian.Hutter@mae.etet.lu)
LV	Martins Nilsons (martins.nilsons@mod.gov.lv)
MT	
NL	
PL	Przemyzlaw Wozniak (pwozniak@mon.gov.pl)
PT	
RO	Sorin Soana (sorin.soana@rpro.eu)
SE	
SI	
SK	
NO	Erlend Hoff (erlend-oby.hoff@fd.dep.no) ; Havard Sandvik (havard.sandvik@fd.dep.no)

Key elements for the call text

This section gathers information in view of the elaboration of a call text.

Specific challenge

Over the last decade, cyber range technologies have matured to a sufficiently developed concept with various technological components that satisfy the basic needs and requirements that both cyber range operators and users have. However, these developments have not relied on innovation per se but rather on implementing more widely used technological concepts and components (e.g. providing useful visualisations, ensuring basic realism for training scenarios, enabling interconnection of different ranges).

The current challenge, however, is to design and develop solutions that deliver notable progress vis-à-vis the current state-of-the-art, including in view of wider technology landscape. This means that focus has to shift from creating cyber ranges that fulfil basic needs to cyber ranges that target next-level capability requirements.

The current challenges focus on the use of cyber ranges for trainings and exercises. The to-be-proposed solutions, however, can benefit also other cyber range use-cases such as product development and penetration testing. Therefore, considerations of such use-cases may be taken into account for developing the solutions.

This next-generation cooperative cyber range capability must address the following challenges:

1. Delivery of trainings and exercises with **classified information,** especially for cross-border exercises by EU Member States and EDF associated countries (Norway).

Although the use of classified information in national exercises and trainings is not a new phenomenon, it is, firstly, still absent from the capabilities of many nations and, secondly, there is no existing solution that offers an EU-wide, cross-border classified capability. Such a capability could help various countries in using this functionality which they otherwise would not be able to use and it would provide a currently unavailable solution to conducting exercises across nations, including for topics such as information sharing and ensuring confidentiality of related data. This would also benefit the EU's military structure, e.g. EU Military Staff, European Defence Agency and others.

Moreover, such a capability can be used by nations internally, e.g. for its different security agencies both in defence and national security to increase interoperability.

2. Delivery of trainings and exercises covering the **entire chain of cyber defence operations** from planning through conduct up to review, including by utilising realistic mission networks.

Most large-scale technical cyber exercises that are currently conducted to not sufficiently cover all relevant aspects of cyberspace operations. While such aspects are sometimes covered in non-technical exercises, these tend to not sufficiently well incorporate technical cyber defence teams. As a result, truly comprehensive and effective exercises are difficult to deliver.

The aspects that surround these technical activities (e.g. operation planning, legal considerations) and which complement incident management (e.g. intelligence activities) require different scenarios and different technical exercise environments in comparison to existing capabilities. The latter also includes the challenge of creating realistic federated mission networks for training purposes.

3. Leveraging **Artificial Intelligence** throughout the delivery of trainings and exercises (e.g. for Blue, Red, White and Green Teams)

The use of AI in different phases and parts of cyber exercises and trainings has been researched and developed to an extent. This includes, for example, AI-based scenario generation (research published by ENISA) and AI-based Red Teams (developed in different private companies). It is clear that AI can assist in these and other parts of cyber capability development. The proposals are expected to provide AI-based solutions that target all major parts of cyber exercise and training delivery.

4. Delivery of trainings and exercises that leverage the concept of **digital twins.**

Digital twins as a concept have a long history. The use of such solutions in cyber exercises has also been targeted previously but not with results that have been sufficiently persistent or useful. Therefore, the challenge remains on developing digital twins or other high-fidelity simulations that have a reasonable cost-effectiveness – given that a common dilemma in such simulations is finding a balance between cost of creating such digital copies and the learning impact that those simulations can offer on top of more standardised ways for IT/OT system and network simulations. One possible avenue for successful balancing of these requirements can be in relation to the space domain, given its increased need for simulations and testing.

Moreover, it is expected (but not mandatory) that the proposals tackle **one or more challenges in addition to the above specifically listed challenges.** Such additional challenges have to:

- align with the expected impacts of the current topic
- be with a comparable level of complexity,
- be clearly different from the specifically listed challenges.

This means that an additional challenge cannot be reasonably considered as being part of a specifically listed challenge.

All solutions must consider the **challenge of sharing and pooling cyber range capabilities** in a coordinated manner between cyber range providers. This challenge may be best addressed by using and enhancing existing initiatives and projects. Moreover, this sharing and pooling can be demonstrated, for example, via the implementation of the project's solutions in different cyber ranges through federation. If federation as an approach is used, it is expected that the proposals cover also the business and management side of the federation. This could, for example, formalise in the development of model cooperation agreements that mimic actual needs and have been developed with processes similar to actual processes.

Where existing or new cyber range and cyber exercise standards (e.g. for scenario development and gamenet creation) are covered, the proposal are expected to address the challenge of achieving a wide user-based of the standard. Proposing the use of any such standards without clearly addressing the way forward may invalidate the whole part of the proposal related to such standards because the success of a standard is as much dependent on the community as the standard's actual content.

Targeted activities

The proposals must cover at least the following tasks as part of the mandatory activities:

- Studies:
  - Identification of additional challenge(s) with a comparable level of complexity as those specifically listed above
  - Definition of capability statements for the solutions to all of the challenges
  - Assessment of the feasibility of achieving the capability as per the capability statements
  - Based on the feasibility assessment, definition of the most appropriate technical requirements for the solutions
- Design:

    - Design of the solutions for each of the specifically listed challenge.
- System prototyping:
    - Development of one or more system prototypes for each of the solution that target the specifically listed challenges.
- Testing
    - Testing of all of the prototypes developed under system prototyping.
    - Testing of one or more system prototypes at least in:
        - 1 new live-fire cyber exercise with 3 or more nations, organised by the consortium
        - 1 existing live-fire cyber exercise with 3 or more nations (e.g. an exercise that is part of a series where at least 1 exercise has been held and where the exercises are held irrespective of the current topic)
- Qualification:
    - Qualification of the system, systems or system components for each of the specifically listed challenge.
- Certification:
    - Certification of the system, systems or system components which are used for the purpose of using classified information
    - Certification of the system, systems or system components which are used for the purpose of delivering complete cyber operations trainings and exercises

Additionally, the proposals should cover the following tasks:

- Design:
    - Desing of the solutions to the additional challenge(s)
- System prototyping:
    - Development of one or more system prototypes for the additional challenge(s)
- Testing:
    - Testing of all of the prototypes in at least 1 live-fire cyber exercise

The proposals may also cover the following tasks:

- Qualification:
    - Qualification of the additional challenge(s) system prototypes
- Certification:
    - Certification of the system, systems or system components which are used for the purpose of leveraging the concept of digital twins
    - Certification of the system, systems or system components which are used for the purpose of leveraging AI
    - Certification of the additional challenge(s) system prototypes

Functional requirements

The proposed products and technologies should meet the following functional requirements:

- Use of classified information
    - [to be extended]
- Delivery of complete cyber operations trainings and exercises
    - [to be extended]

- Leverage AI
    - AI-based Red Team
    - Use of AI-based Blue Team tools and agents but also AI-based gamenet components (e.g. an AI-based technology or application that is used in everyday cyber defence and security operations)
    - Use of AI-based solutions for user simulation and/or other aspects that create “noise” and add depth and breadth to the exercise environment
    - Use of AI-based tools for training and exercise delivery (e.g. by Green and White Teams in creating scenarios and building gamenets, including dynamic amendments during training delivery)
    - [to be extended]
- Leverage digital twins
    - [to be extended]
- Sharing and pooling of capabilities
    - Solutions to all challenges must contain functionalities for sharing and pooling. For example, through concepts such as federations, marketplaces and common scenario creation standards.
    - [to be extended]
- [to be extended]

Expected impacts

The outcome should contribute to:

- a stronger, more competitive and technologically independent European Defence Technological and Industrial Base (EDTIB) when it comes to solutions for cyber defence training and exercising;
- improved interoperability and future capabilities of EU Member States and EDF associated countries (Norway) forces in the area of cyber defence for cyber mission planning and execution, including through the use of classified information and high-fidelity simulations such as digital twins within the training process;
- improved interoperability between civil and military actors both within EU Member States and EDF associated countries (Norway) and across those nations
- better cooperation of EU Member States and EDF associated countries (Norway), research and industrial actors towards defining a common vision on cyber capability development.

Needed follow-on

This section gathers information on further EDF funding needs for follow-on actions if applicable. The information should be suitable for inclusion in a multiannual perspective.

As of now, there is no expectation for further EDF funding needs for follow-on actions.