EUROPEAN DEFENCE AGENCY

FACT SHEET

www.eda.europa.eu

CYBER RANGES FEDERATION PROJECT

To secure and exploit all the opportunities offered by cyberspace (commonly considered as the fifth domain of warfare), disposing of a highly skilled and well-trained personnel specialised in the cyber domain and having the ability to test and verify cyber defence-related equipment is crucial for any cyber defence capability.

Background

The importance of cyber range facilities in support of training and exercises was recognised in the 2014 Capability Development Plan (CDP) as an important capability gap that needs to be urgently tackled. It was also observed that, while many Member States were already building military cyber ranges, their efficiency would depend on their ability to cover the full scope of simulation activities and provide a realistic and effective experience to users. However, the complexity of the cyberspace, the wide range of attack vectors and many other factors made it very difficult to concentrate the full scope of activities into a single cyber range. Consequently, in May 2017, EDA launched the Cyber Ranges Federation project which aims to pool and share existing cyber ranges capabilities between Member States. The project currently has eight participating Member States (pMS), namely Austria, Belgium, Estonia, Finland, Germany, Italy, Latvia and Sweden.

The cyber ranges participating in the project are multi-purpose environments supporting three primary processes: (1) education, training and exercises (ETE); (2) asset test and risk analysis; and (3) cyber defence exercises and knowledge sharing. The project objective is to develop a sophisticated and powerful platform at European level not by building a new cyber range, but instead by interconnecting Member States' national cyber defence exercises communities (including countries that do not have their own cyber ranges), in order to allow each of the participating members to train and further improve their respective cyber defence skills as well as to enhance the functionalities and capacities of existing, emerging and future cyber ranges.

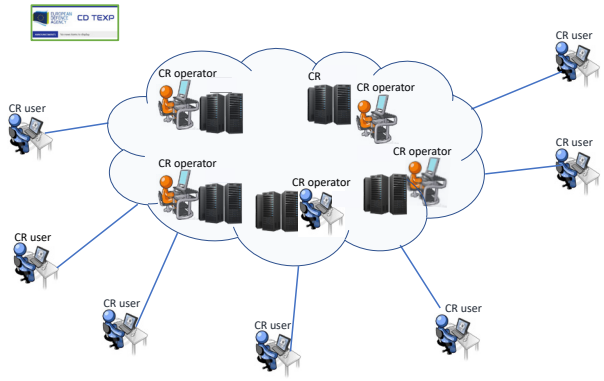
The specificity and relevance of the project reside in the fact that it is one of the first European initiatives aiming to **join existing national cyber ranges together and create a supportive community**. The establishment of such a community allows for the sharing of information, knowledge and experience on the development, establishment and operation of cyber ranges. The project success relies on the community built around the project which, on the one hand, developed and implemented the project features and, on the other hand, uses the developed training and exercise features in accordance with a Memorandum of Understanding also developed by the project.

During the project's first phase , between 2017 and 2019, a technical architecture as well as a support community (including a legal and operational governance model) were developed, all based on technical requirements for cyber training and exercise platforms. The project also performed a series of market studies and a review of the related state-of-the-art technologies. This phase ended with a live multinational demonstration exercise held in Helsinki, Finland in November 2019 during the EDA Project Team Cyber Defence Meeting, showcasing the practical implications and benefits of connecting and jointly using Member States' cyber ranges to improve and expand their cyber training capabilities.

State of Play

Project phase 2 started in 2020 and introduced the concept of multiple sub-projects, a more effective mechanism to achieve additional benefits of the project. Three sub-projects are ongoing. The first one is focused on creating a business case for the use of Artificial Intelligence (AI) in cyber defence exercises. The second one aims at introducing an exercise formal definition language and related automation to simplify an exercise scenario deployment and make it more efficient and effective. The third one focuses on creating a federated situational awareness and scoring service, to provide more effective situational awareness during the execution of an exercise, and also introduce a semi-automated mechanism for scoring and assessing exercise participation.

Cyber Ranges federation Envisioned End-state



Way ahead

The project continues to further develop Phase 2, by implementing current sub-projects and creating new ones under the guidance of the Member States-led project management committee. Sub-project 1 on AI in cyber exercises, in particular, is aiming at defining a follow-on project, implementing one of the scenarios defined in the business case.

The Cyber Ranges Federation will also use its platform (and its community) to participate in more cyber training events with the aim to increase the sharing of knowledge and best practices as well as its visibility, such as with the milCERTs Interoperability Conference (MIC).