Cyber Ranges: EDA's First Ever Cyber Defence Pooling & Sharing Project Launched By 11 Member States

On May 5th, the Project Arrangement (PA) for the first ever Cyber Defence Pooling & Sharing Project was signed by all eleven contributing Member States. The Cyber Ranges Federation Project brings together Austria, Belgium, Germany, Estonia, Greece, Finland, Ireland, Latvia, the Netherlands, Portugal and Sweden under the co-lead of the Netherlands, Finland and Greece. The project originates from an EDA initiative and will be carried out under the EU pooling & sharing agenda with support from EDA. The core aims of the project include: increasing the availability of existing and emerging cyber range facilities; increasing the occupation rate and efficiency of cyber ranges and platforms; mainstream and improve cyber defence training, exercises and testing at European level. Under this PA, the objectives will be achieved in a spiral approach over the next 36 months.

The Cyber Ranges Federation Project is the first of four Cyber Defence Projects launched so far under the Pooling & Sharing agenda. While other projects such as Improved Cyber Situation Awareness, improved Advanced Persistent Threat (APT) detection, and pooling of Member States' demand for private sector-provided cyber training are still in the preparation phase, the Cyber Ranges Federation Project is the first cyber defence related collaborative EDA project that is moving from the preparation phase to the implementation phase.

A total of 30 work packages are foreseen for the project, divided between two spirals. Work on the first spiral, composed of 19 different work packages, will commence with the first meeting of the Project Management Committee under the lead of the Netherlands. Spiral 1 is expected to be completed within 18 months. The remaining 11 work packages will be completed after a review of the results of spiral 1 under the lead of Finland in spiral 2. It is expected that the projects will substantially contribute to improving the quality and authenticity of cyber defence related education, training and exercise formats for all stakeholders in Europe. This will be achieved by providing on the one hand wide ranging and capable technical platforms and on the other by establishing a European community of experts on up-to-date cyber defence training and exercises.

The sharing of knowledge and best practice is also an implicit objective of the project. In doing so, the Cyber Ranges Federation will also be supported by an EDA developed web-based Cyber Defence Training and Exercise Coordination Platform (CD TEXP), which is expected to be operational by the end of this year. In addition to training and exercise support, the cyber ranges can also be effectively employed in the areas of research as well as modelling, simulation and testing. Project preparation was observed by NATO, and in the light of the NATO-EU Joint Declaration, additional ways for cooperation with the project of NATO to establish its own cyber range capacity will be sought by the contributing Member States.

Background

The success of military operations, including EU-led operations, is increasingly dependent on the availability of, and access to, cyberspace. The EU Cyber Security Strategy 2013 recognizes Cyber Defence as one of the strategic priorities of the EU and Heads of State and Governments decided in December 2013 that Cyber Defence should be one of four key areas for capability development. An essential element of EU cyber defence capability is highly skilled and well-trained personnel. Enhancing awareness and education of technicians, operators and decision-makers is urgent. Cyber ranges to support training and exercises are both essential and scarce. In the 2014 Capability Development Plan, the scarceness of cyber range facilities in support of Training and Exercises was recognized as an important capability gap that urgently needs resolution. The now established project serves to close this capability gap. Pooling & Sharing projects are an integral means for closing capability gaps in the cyber domain.

More information: