EUROPEAN DEFENCE AGENCY

FACT SHEET

www.eda.europa.eu

EDA CYBER DEFENCE PROGRAMME

Cyberspace is regarded as the fifth domain of warfare, together with land, air, maritime and space. Armed Forces increasingly rely on the ability to operate in cyberspace across the entire spectrum of cyber operations.

Context

In November 2014, the European Council adopted a Cyber Defence Policy Framework (CDPF) which was reviewed and updated in November 2018 to include the following priorities related to Member States and EU entities' cyber defence capabilities: (1) promotion of civil-military cooperation and synergies; (2) improvement of training, education and exercises opportunities; and (3) cooperation with relevant international partners. These priorities were further developed by the EU defence community: in the EU Capability Development Plan (CDP) revision of June 2018, Member States identified "Enabling Capabilities for Cyber Responsive Operations" as one of the 11 European capability development priorities, highlighting the growing importance of cyber defence in Europe's capability landscape. The CDP priorities were further finetuned into Strategic Context Cases (SCC), supporting the implementation of the priorities. The SCC on "Enabling Capabilities for Cyber Responsive Operations" addresses this priority by proposing five modules (described below) through which EDA and its Member States should approach capability development in the cyber domain. These EDA modules are fully in line with and support the new EU Cyber Security Strategy, released by the EU Commission and the European External Action Service (EEAS) in December 2020, which emphasises that the EU and its Member States should provide further impetus for the development of state-of-the-art cyber defence capabilities.

Cyber cooperation and synergies

Cooperation between different actors is a key pillar for increased resilience against cyber threats. It aims to achieve synergies through joint efforts by both civil and military stakeholders (including NATO entities under the remit of the EU-NATO Joint Declaration of July 2016 and its update from 2018).

Cyber research and technology

EDA conducts several cyber research and technology (R&T) activities to develop technologies that are essential to counter cybersecurity threats.

As part of EDA's Overarching Strategic Research Agenda (OSRA), the Cyber Defence Strategic Research Agenda (SRA) aims to target research & technology efforts on specific military aspects and will include an R&T roadmap for the coming years.

Systems engineering framework for cyber operations

This EDA activity aims to create a standardised and interoperable systems engineering approach to support the harmonisation of requirements for cyber defence capabilities across the Member States, with the long-term goal of creating an enterprise architecture for cyber responsive operations.

Cyber education and training

Pooling and sharing of training and exercises, thus creating a more efficient and effective workforce, is a key success factor for cyber defence. EDA develops and runs pilot courses and exercises for new training formats and delivers a variety of new cybersecurity & defence courses, based on the results of a 2020 analysis into the training needs in this domain. After that, a "Methodology for Developing Cyber Defence Training Courses" was delivered to Member States to assist the development, delivery and evaluation of cyber defence pilot courses.

Specific cyber defence challenges in the air, space, maritime and land domains

As cyberspace is a transversal domain, it is crucial to also consider the implications it has on the other operational domains, namely air, land, maritime and space. To achieve this, EDA aims to identify and assess concrete cyber defence challenges in these domains.

The Agency will work on the identification of cyber defence requirements for all information infrastructures and systems used in the different domains, including legacy command & control systems as well as new ones, with the aim to harmonise cyber defence techniques and solutions across the systems used in the various domains, and improve the cyber-resilience of mission-critical systems.

Projects

EDA projects developed under the Cyber Defence SCC can be divided into two categories: EU cooperation projects and EDA projects.

EU cooperation projects

- EDA, the EU Cybersecurity Agency (ENISA), Europol's European Cybercrime Centre (EC3) and the Computer Emergency Response Team for the EU Institutions, Agencies and Bodies (CERT-EU) signed in May 2018 a Memorandum of Understanding (MoU) to establish a cooperation framework by exchanging expertise and best practices in cyberspace.

- EDA closely cooperates with NATO, including Allied Command Transformation, the NATO Communications and Information Agency (NCIA) and the Cooperative Cyber Defence Centre of Excellence (CCD COE). Activities focus on the exchange of information and program alignment, always avoiding unnecessary duplication of efforts and resources.

- Together with the EU Military Staff, EDA contributes to the cyber defence focus area of the US-led Multinational Capability Development Campaign (MCDC).

- The Cyber Ranges Federation project aims at improving the effectiveness of Member States' investment in national cyber ranges by developing a federated infrastructure for cyber training purposes at European level, as a result of interconnecting existing capabilities.

- The deployable Cyber Situation Awareness Package (CySAP) for headquarters project aims to integrate cyber defence in the conduct of military operations and missions and to provide a common and standardised cyber defence planning and management platform.

- EDA also works on the MASFAD II (Multi-Agent System For Advanced persistent threats Detection) project which develops a capability able to manage and prevent intrusions by sophisticated actors targeting governments and their institutions.

EDA projects

- The Cybersecurity of Supply Chain project focuses on creating a risk management model for cybersecurity risks posed to military capabilities by the supply chain used to develop and use them.

- The milCERTs Interoperability Conference is a conference format designed to bring together military CERTs and identify and address gaps in their interaction while managing large cyber defence incidents affecting the EU.

- The current version of the Enterprise Architecture Framework, CyDRE (Cyber Defence Requirements Engineering), aims to harmonize the design and development of national cyber defence capabilities following a shared vision, in order to avoid uncoordinated efforts, applications, services, standards, vocabularies and taxonomies.

- The Cyber Defence Training & Exercises Coordination Platform (CD TEXP) offers a collaborative platform at European level for browsing and booking training opportunities.

- The Cyber Awareness Train-the-Trainers pilot course aims to build a network of EU and national cyber awareness trainers and to improve interoperability.

- The Cyber Strategic Decision-Making exercise trains key governmental actors in Member States to face and manage cyber crises in a hybrid context.

- The Cyber Phalanx is a combined course and exercise for operation planners to raise their awareness regarding cyber and hybrid threats in the Operations Planning Process (OPP) on both strategic and operational levels.

Updated: 5 July 2021