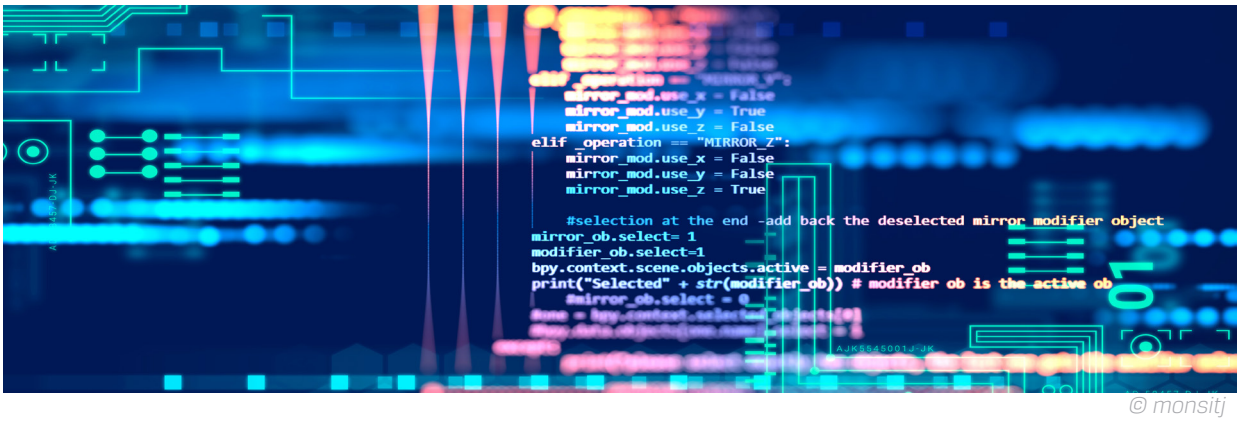
EUROPEAN DEFENCE AGENCY

Fact sheet

www.eda.europa.eu

Cyber Defence



© monsitj

Cyberspace is understood as the fifth domain of warfare equally critical to military operations as land, sea, air, and space. Success of military operations in the physical domains is increasingly dependent on the availability of, and access to, cyberspace. The armed forces are reliant on cyberspace both as a user and as a domain to achieve defence and security missions.

The Cyber Security Strategy for the European Union (EU), which was released in February 2013 and endorsed by the Council in June 2013, emphasises, "Cyber security efforts in the EU also involve the cyber defence dimension." Consequently, the European Council adopted a "Cyber Defence Policy Framework (CDPF)" in November 2014, highlighting five priorities:

- Supporting the development of Member States' cyber defence capabilities related to Common Security and Defence Policy (CSDP);
- Enhancing the protection of CSDP communication networks used by EU entities;
- Promotion of civil-military cooperation and synergies with wider EU cyber policies, relevant EU institutions and agencies as well as with the private sector;
- Improve training, education and exercises opportunities;
- Enhancing cooperation with relevant international partners.

In the European Defence Agency (EDA) Capability Development Plan (CDP), cyber defence is one of the priority actions. A Project Team of EDA's participating Member States' representatives is responsible for jointly developing cyber defence capabilities within the CSDP. A Cyber Research and Technology working group supports this work with collaborative activities delivering the required technologies at the right time. All of this is positioned next to existing and planned efforts by civil communities (national and EU institutions) and NATO within the remit of the EU-NATO Joint Declaration of July 2016. Given that threats are multifaceted, a comprehensive approach that fosters cooperation between the civil and military Communities of Interest (CoI) in protecting critical cyber assets is the key enabler for these synergies. In this context, the EDA, the European Union Agency for Network and Information Security (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 the areas of cyber security, cyber defence and investigating cybercrime.

EDA Cyber Defence Projects

The Agency is active in the fields of cyber defence capability development and in Research & Technology (R&T). In accordance with the 2018 Capability Development Plan Revision the focus is on:

Enabling capabilities on cyber responsive operation by addressing.

a. Cyber cooperation and synergies;
b. Cyber Research and Technology;
c. Systems engineering framework for cyber operations;
d. Cyber education and training;
e. Specific cyber defence challenges in the air, space, maritime and land domain.

Training & Exercises

Following a structured cyber defence training need analysis, which is expected to be updated by the end of 2019, EDA develops, pilots and delivers a variety of cyber security & defence courses from basic awareness over expert level to decision maker training. This is accompanied by exercise formats for comprehensive cyber strategic decision-making and cyber defence planning for headquarters. In the future, pooling and sharing of training and exercises will be facilitated at European level by an EDA developed collaborative platform, the Cyber Defence Training & Exercises Coordination Platform (CD TEXP).

Member States' collaborative project ideas include the increasing mutual availability of virtual cyber defence training and exercise ranges (Cyber Ranges) for national cyber defence specialists' training. The ranges are multi-purpose environments supporting three primary processes: knowledge development, assurance and dissemination. Accordingly, a federation of ranges may leverage three complementary functionality packages: Cyber Training & Exercise Range, Cyber Research Range as well as Cyber Simulation & Test Range functionalities.

Cyber Situation Awareness

EDA is working on cyber defence situation awareness for CSDP operations and how to integrate cyber defence in the conduct of military operations and missions. The aim of the deployable Cyber Situation Awareness Package (CySAP) for headquarters project is to integrate these functions and to provide a common and standardised cyber defence planning and management platform, that allows military commanders and their staff to fulfil cyber defence related tasks in their day-to-day business. Together with the EU Military Staff, the Agency actively contributes to the cyber defence focus area of the US-led Multinational Capability Development Campaign (MCDC).

Advanced Persistent Threats (APT) Detection

Governments and their institutions are among the most prominent targets for APT malware, mostly aiming at cyber espionage. Intrusions are either discovered too late or not at all. Early detection is crucial to properly manage the risk imposed by APT. After a very successful feasibility demonstrator EDA is leading a follow-on project with a group of interested Member States to develop an even more capable solution as an operational prototype.

Digital Forensics for Military Use

The collection and evaluation of digital evidence in a military context becomes more and more important, in order to learn lessons from previous attacks (Post-Mortem Analysis), to attribute attacks to perpetrators, to harden military information infrastructures and to improve online analysis capabilities (Ante-Mortem Analysis). The EDA project for a Deployable Cyber Evidence Collection and Evaluation Capacity (DCEC2) develops a technical demonstrator for a digital forensics capability for the military that specifically responds to the requirements of deployed military operations, such as force protection, agility and rapidity.

Cyber Defence Strategic Research Agenda (SRA)

Cyber security technologies are relevant to both the civil and the military domain ("dual-use"). Considering on-going and future civil research, for example within the EU Research Framework Programmes, and the high resilience required in defence, it will be crucial to precisely target research & technology (R&T) efforts on specific military aspects. The Cyber Defence SRA is considering these aspects and will include a R&T roadmap for the coming years. It will be part of an Overarching Strategic Research Agenda (OSRA) for the military and will be aligned and delineated with other research agendas in the cyber security & defence domain. Coordination of research projects with other EU stakeholders such as the European Commission, the European Space Agency and the European Cyber Security Organisation is also implemented.