EUROPEAN DEFENCE AGENCY

Fact sheet

www.eda.europa.eu

Cyber Defence

Introduction

Cyberspace today is often described 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, 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" in November 2014, highlighting five priorities:

- Supporting the development of Member States' cyber defence capabilities related to 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, cyber defence is one of the priority actions. A project team of EDA and its participating Member States' representatives is responsible for jointly developing cyber defence capabilities within the EU common security and defence policy (CSDP). A network of EDA and Member States research & technology experts support this work by 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. Given that threats are multifaceted, a comprehensive approach is taken, seeking to enhance synergies between the civilian and military domains in protecting critical cyber assets.

EDA Cyber Defence Projects

The Agency is active in the fields of cyber defence capabilities and in the research & technology domain.

Training & Exercises

Following a structured cyber defence training need analysis, EDA has delivered a variety of cyber security & defence courses from expert level to decision maker training and exercises. In the future, pooling and sharing of training and exercises will be facilitated even more, by building a collaborative platform and creating a "market place".

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.

Cyber Situational Awareness

EDA is currently also working on cyber defence situational awareness for CSDP operations and how to integrate cyber defence in the military operational planning process. For both aspects EDA is together with the EU Military Staff actively contributing to the cyber defence focus area of the US-led Multinational Capability Development Campaign. The aim of the deployable Cyber Situational Awareness Package (CySAP) for headquarters ad hoc project is to integrate these functions and to provide a common and standardised cyber defence planning and management platform, that allows Commanders and their staff to fulfil the cyber defence related tasks in their day-to-day business and throughout all phases of an operation.

Cyber Defence Research Agenda (CDRA)

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 Programme, and the high resilience required in defence, it will be crucial to precisely target research & technology (R&T) efforts on specific military aspects. The CDRA is considering these

aspects and includes a R&T roadmap for the coming 10 years. Coordination of research projects with other EU stakeholders such as the European Commission and the European Space Agency is implemented under the European Framework Cooperation.

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 for a concept to properly manage the risk imposed by APT. Consequently, EDA is leading a project to develop possible solutions.

Protection of Information, Cryptography

Academia in Europe have been able to build up and network extraordinary skills in cryptology over the past years. Technology trends such as smart systems or Internet of Things require very high information protection, both for safety and security. It will be crucial to transfer the academic knowledge on crypto into innovative products, also for military use. Since this is a multi-facetted challenge involving a series of stakeholders, consultations have started under the umbrella of the European Framework Cooperation.

Last update: 10 February 2015