EUROPEAN DEFENCE AGENCY

Fact sheet

www.eda.europa.eu

Cyber Defence

Introduction

Cyberspace today is often described as the fifth dimension of warfare equally critical to military operations as land, sea, air, and space. Success of military operations in the physical domains is more and more depending 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 therefore emphasises, "Cybersecurity efforts in the EU also involve the cyber defence dimension."

Cyber defence is one of the ten priorities in the European Defence Agency (EDA) capability development plan (CDP). A project team of EDA and its participating Member States' (pMS) representatives is responsible to jointly develop these cyber defence capabilities within the EU common security and defence policy (CSDP). A network of EDA and MS research & technology (R&T) 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 stocktaking study

Objective & methodology

EDA commissioned an one-year study to establish an in-depth understanding of cyber defence capabilities across EDA MS to support progress towards a more consistent level of cyber defence capability across the EU. 20 countries participated in the study.

This stocktaking exercise included research into the different EU level organisations involved in cyber-defence activities in the context of CSDP missions as well as data collection on cyber defence capabilities in each Member State. The research was carried out via document review, semi-structured interviews and the development of a questionnaire distributed to those EU Member States participating in the EDA's Cyber Defence Project Team.

Cyber defence capability information was analysed according to a commonly understood military framework of functional contributors to defence capability, known as Defence Lines of Development (DLoDs). These contributors are: doctrine, organisation, training, material, leadership, facilities and interoperability (DOTMLPF-I). To measure and to a certain degree benchmark the degree of "Cyber-Readiness" the study utilised a five step maturity model with 69 discrete and weighted indicators for maturity; broken down within the DOTMLPF-I structure to achieve the required granularity. Each country was qualitatively assessed in each contributor against this weighted maturity model. The study report including an unclassified summary was presented in May 2013. Profiles for each participating Member State (pMS) are provided in the classified report.

Results

The study finds a complex and diverse picture with regard to cyber defence capability at both the EU level and within the pMS.

As for cyber defence among EU organisations, the study highlights the complex operational set-up between European Defence Agency, European External Action Service (EEAS), General Secretariat of the EU Council and European Commission and related EU agencies like the European Network and Information Security Agency (ENISA), the European Cybercrime Centre (EC3) and the Computer Emergency Response Team (CERT-EU). While threat analysis and cyber-intelligence gathering capability appears to be emergent, incident response capabilities could be deepened. The study also reveals that the culture of cyber-security good practice needs to be nurtured and that the use of military specific standards and tools is still poorly understood.

For MS a mixed picture with respect to military cyber defence capability was detected. Generally speaking, MS in which key decision-makers are familiar with cyber-security, cyber defence capabilities are more advanced. The 20 MS exhibit strengths in the three capability domains Leadership, Personnel and Interoperability. In the areas of Doctrine, Organisation and Training, an early level of maturity was defined which might be linked to the fact that these three areas require more complex and longer-term efforts to establish organisational structures. Facilities is the capability domain which remains to date highly immature or non-existent.

Recommendations

EU level

Military cyber defence in the EU is at a relatively early stage of maturity. Therefore, the recommendations issued in the study are tentative high-level aspects to consider as cyber defence at the EU level evolves and they are detailed in more depth in the classified report of the study:

- Enhancing EU network protection for example through centralised management of data exchanging networks
- Strengthening intelligence capability for example through the development of a cooperation model with other actors like EC3 and ENISA
- Deepening incident response capabilities for example through

improved warning and alert mechanisms

• Creating a culture of cyber security (good practice, training and awareness-raising) for example through a pan-institutional cyber security task force

• Promulgating security standards and tools like for example the ISO2700x suite and future standard setting in negotiation with NATO

• Reinforcing links between NATO and the EU for cyber defence issues for example through NATO-EU joint exercises and joint cyber crisis management mechanisms

For MS

• MS should be encouraged to develop their cyber defence doctrine in close coordination with the other pMS

• A watching brief should be kept on how organisational structures evolve to ensure a coordinated response in each MS

• Greater attention should be given to the development of cyber defence training and education initiatives, both at the operational and senior command levels

• MS could consider exchanging information on equipment solutions and pooling and sharing for cyber defence capabilities, especially in EU-led missions

• Exchange of information on practice for the recruitment and retention of cyber defence specialists would be helpful for example through "Cyber Reserve Forces"

• Processes and shared escalation procedures could be exchanged and developed to execute leadership in cyber defence, especially in the context of EU-led operations

• MS could consider to a certain extent sharing facilities and what services are offered within them for example for forensic facilities

• Greater consideration needs to be paid to the interoperability aspects of cyber defence, especially with non-military organisations.

Next steps

The results of the study are currently under evaluation with pMS and EDA expects many actions to be derived from the study recommendations, especially in areas where pMS benefit from closer cooperation. However, some recommendations are already taken for action, especially in the area of training and exercises clearly aiming on building a European Cyber Defence Culture (see below).

EDA Cyber Defence Projects

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

Training

EDA is currently conducting a structured Cyber Defence Training Need Analysis (TNA) in order to build a Cyber Defence Training Curriculum. The TNA builds on existing training capacities in pMS and EU institutions and is done also in close cooperation with the Cooperative Cyber Defence Center of Excellence in Tallinn. Also the first collaborative project has been identified and will be formalised soon. This project aims at increasing the availability of virtual cyber defence training and exercise ranges (Cyber Ranges) for pMS cyber defence specialists training.

Situational Awareness (Kits)

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 EUMS actively contributing to the Cyber Defence Focus Area of the US-led Multinational Capability Development Campaign (MCDC). The aim of the deployable Cyber Situational Awareness kit (Cyber SA kit) for operational/force headquarters ad hoc project initiative is to integrate these functions and to provide a common and standardised cyber defence planning and management platform, that allows Commanders and their staff in EU-led operations to fulfil the cyber defence related tasks throughout all phases of an EU-led operation.

Cyber Defence Research Agenda (CDRA)

Cyber security technologies are clearly relevant to both the civil and the military domain ("dual-use"). With the civil research already performed and further planned for example within the EU Research Framework Programme, and the limited financial resources in defence, it will be crucial to precisely target R&T efforts on specific military aspects. The CDRA will consider these aspects and propose an R&T roadmap for the coming 10 years.

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 preparing a call for proposals for first analysis and ideas of possible solutions.

Technical Forum for Cyber Defence Technologies

The R&T forum "IAP4" (related to communication and information technology – ICT) gives pMS a platform to discuss and prepare collaborative R&T projects on cyber defence. While a number of such proposals is expected from the CDRA roadmap, the requirement of cooperation in cyber defence modelling and simulation (M&S) is already visible now.