© Leonardo

CYBER DEFENCE SITUATION AWARENESS PACKAGE - RAPID RESEARCH PROTOTYPE (CYSAP-RRP)

In 2013, EDA's Project Team Cyber Defence (PT CD) identified the need for capabilities that would enable military commanders at all operational levels to understand and manage the risk of cyber-attacks.

EDA started to work on Cyber Situational Awareness acknowledging that available solutions on the market at that time were not (and still are not today) able to fulfil the entire spectrum of requirements of military commanders. This is especially true with respect to:

1. deployability

2. capturing, displaying and assessing the status of own, continuously transforming static, deployed and mobile CIS

3. risk analysis including mission impact analysis

4. cyber related courses of action analysis, and

5. decision making support.

An important prerequisite for dynamic cyber risk management is to provide the commander and his staff with real-time situational awareness , based on both generic and specific threat scenarios, from which the risk of cyber-attacks can be observed, understood, and evaluated.

The objective is for military commanders to have a clear understanding of the cyber threat landscape including system vulnerabilities and attack vectors, and to equip them with the tools required to make informed decisions to manage cyber risks during the planning and conduct phases of an operation. In 2014, a dedicated Cyber Defence Situation Awareness Package (CySAP) ad hoc working group comprising the contributing Member States, EDA and additional subject matter experts and stakeholders started to work on a Common Staff Target (CST), Common Staff Requirements (CSR) and a business case which describes theoperational elements needed to achieve such a cyber situational awareness for EU Member States' Armed Forces. The objective of the working group was to initiate preparations for an EDA ad hoc project. The project arrangement for developing a "Cyber Defence Situation Awareness Package- Rapid Research Prototype (CySAP-RRP)" was signed end of 2018 by three contributing Member States; Spain (lead country), Germany and Italy. A European industry consortium comprising INDRA Sistemas SA, Leonardo S.p.a., and Fraunhofer FKIE was selected to support and execute the project. The core objectives of the project included essential research challenges to assist military decision-makers in cyberspace. The project results were delivered over a 20 months period including final testing of the prototype in November 2020.

Cyber Situation Awareness - spearhead of technological innovation

The CySAP-RRP was built upon previous work done by EDA to develop a target architecture and system requirements for an enhanced cyber defence situation awareness capability. CySAP is a technology demonstrated in a laboratory and an initial attempt to provide military commanders with an understanding of the situation in cyberspace. It feedsoperational cyber aspects into mission commanders' decision-making. It is a software-based solution integrated into a platform with various interfaces linked to different sources of information.

CySAP is at the forefront of technological efforts aiming to obtain a 'common and standardised cyber defence planning and management functional area service' for Armed Forces in Europe. The research challenges were to provide a comprehensive integration of cyber defence elements into the planning and execution processes of military operations. CySAP will guide future developments in this field and is considered essential for achieving a fully-fledged command and control capability for cyber operations. CySAP follows a modular approach with a mix of functionalities that can be called upon to meet operations' particular requirements including decision-making support functionalities, allowing each module to have a stand-alone utility as well as the ability to coherently interoperate. The adopted situational awareness capability architecture will influence additional cyber defence solutions to achieve interoperability. CySAP is designed to operate in full complementarity with a Security Operation Centre (SOC).

What CySAP offers to military commanders in the planning and execution phases of cyber operations

Contributing Member States recognised the urgency of developing specific functionalities - tailored to military needs - into a modular and scalable prototype. The objective is for commanders to have a clear understanding of the operations-specific and real-time threat landscape applied to the communications and information systems (CIS) supporting military operations, be it in the Common Security and Defence Policy (CSDP) context or any other frameworks. It aims to equip the commander with tools and procedures to identify and manage cyber risks during the planning and execution phases of an operation. This should primarily result in well-informed decision-making. Technology foresight activities concentrate on enhancing data processing techniques by using innovative knowledge, cognitive and learning systems. CySAP aggregates a cyber situation analysis that can be seamlessly integrated into an overall common operational picture (COP). This allows for a meaningful representation of the information contributing to producing a timely and accurate overall situation awareness of the mission environment. CySAP is a key aspect in all cyber defence efforts and initiatives currently pursued within the EU and other international organisations.

Background

Cyberspace is the fifth domain of operations, alongside the physical domains of land, sea, air, and space; the successful implementation of EU missions and operations is increasingly dependent on uninterrupted access to a secure cyberspace, and thus requires robust and resilient cyber operational capabilities.

The updated EU Capability Development Plan (CDP) endorsed by the EDA Steering Board in June 2018 reconfirmed cyber defence as a priority for capability development in the EU. The CDP recognises the need for defensive cyber operations in any operational context, based on sophisticated current and predictive cyberspace situational awareness. This includes the ability to combine large amounts of data and intelligence from numerous sources in support of rapid decision making and increased automation of the data gathering, analysis and decision-support process.

In November 2018, the European Council adopted an updated version of the EU cyber defence policy framework (CDPF). Supporting the development of Member States' cyber defence capabilities is a priority area where the now concluded CySAP project serves as a core element to guide future research and operational capabilities. "The EU's Cybersecurity Strategy for the Digital Decade" presented in December 2020 aims to boost cyber defence capabilities and calls the EU and Member States to provide further impetus for the development of state-of-the-art cyber defence capabilities. It also stresses "...the EU lacks collective situational awareness of cyber threats...". CYSAP is one important building block to close this gap in a comprehensive manner.