EUROPEAN
DEFENCE
AGENCY

CYBER DEFENCE

Built on European cooperation

#EUdefence

More information on the European Defence Agency
is available at www.eda.europa.eu

Responsible editor: Elisabeth Schoeffmann, EDA
Printed in Belgium

Introduction

After land, sea, air and space, cyberspace has become the fifth domain of warfare. Armed Forces increasingly rely on the ability to operate in cyberspace across the entire spectrum of cyber operations.

The first time cyber defence has been identified and selected as one of the prioritised actions for capability improvement in the EU framework was in 2010 in the framework of the updated Capability Development Plan (CDP) for Common Security and Defence Policy (CSDP). Since then the European Defence Agency (EDA) has been active in the field of capability development as well as Research and Technology (R&T) for cyber defence capabilities in support of EDA participating Member States.

Based on the first EU Cybersecurity Strategy from February 2013, the European Council adopted a Cyber Defence Policy Framework (CDPF) in November 2014, 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 revision of June 2018, Member States identified "Enabling Capabilities for Cyber Responsive Operations" as one of the 11 European capability development priorities, highlighting and reconfirming 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 within five modules Avenues of Approach through which EDA and its Member States should implement capability development in the cyber domain.

These EDA modules are addressed in the brochure, where the main ongoing cyber-related activities are briefly presented. The modules are fully in line with and support the new EU Cybersecurity 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.

Who we are and what we do

MISSION

EDA was established under a Joint Action of the Council of Ministers on 12 July, 2004, "to support the Member States and the Council in their effort to improve European defence capabilities in the field of crisis management and to sustain the European Security and Defence Policy as it stands now and develops in the future".

WHAT WE DO

EDA supports its 26 Member States in improving their defence capabilities through European cooperation. Acting as an enabler and facilitator for Ministries of Defence willing to engage in collaborative capability projects, the Agency has become the 'hub' for European defence cooperation.

Member States use EDA as an intergovernmental expert platform where their collaborative projects are supported, facilitated, and implemented. Member States can decide on a case-by-case basis whether to participate in projects, depending on their needs and interests. The core of what we do is offering a level of expertise and activities that cover the whole spectrum of defence cooperation. For more information on the work of the Agency, visit our website at www.eda.europa.eu

Cyber Cooperation and Synergies

Fostering cooperation and synergies in the cyber domain has been identified as one of the modules to improve cyber defence capabilities of Member States. Cybersecurity and cyber defence require cooperation between public and private sectors, primarily in terms of sharing information and exchanging best practices. Trust is essential at all levels to create the right environment for the sharing of sensitive information across borders. Poor coordination leads to fragmentation, duplication of efforts and dilution of expertise.

EU MILCERT NETWORK ESTABLISHMENT

Members: More than 20 participating Member States, partners, and organisations.

Objectives: EU Member States have been working on creating Computer Emergency Response Teams (CERT) or Computer Security Incident Response Teams (CSIRT) for several years. Both civilian and military CERT have been created in various venues, formats, capacities, missions and located in various parts of government structures. Many stakeholders have identified the need to extend best information-sharing practices to military CERTs and their operations. The main objective is to use existing scarce resources and structures, create a circle of trust between the milCERT community through a yearly exercise at technical/operational levels to increase training, interconnection and thorough implementation of lessons learned.

CYBER RANGES FEDERATION

Participating members and observers:

🇦🇹 🇧🇪 🇪🇪 🇫🇮 🇩🇪 🇮🇹 🇱🇻 🇸🇪 🇳🇱 🇵🇹 esa

The Cyber Ranges Federation project is one of the first European initiatives aiming to join existing national cyber ranges together and creating a supportive community. It has thus become a sophisticated and powerful platform at European level not by building a new cyber range, but instead by interconnecting Member States' national cyber defence exercise communities. Therefore, allowing the participating members to train and further improve their respective cyber defence skills as well as to enhance the functionalities and capacities of existing, emerging and future cyber ranges.

Systems Engineering Framework for Cyber Operations

The second module within the context of implementing EDA's CDP relates to the creation of a dedicated systems engineering framework for cyber operations: the reference Enterprise Architecture for cyberspace operations.

CYBER DEFENCE REQUIREMENTS ENGINEERING (CYDRE)

A systems engineering framework is a common environment that provides an integrated, traceable analysis capability throughout the life cycle of a programme. It provides an essential supporting structure that enables an iterative collaborative environment for all stakeholders, practitioners and decision-makers to proactively engage in and facilitate decision making. The current version of the Enterprise Architecture framework, CyDRE (Cyber Defence Requirements Engineering), aims to harmonise 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. This framework includes scopes, functionalities and requirements used in the domain by Member States upon national and EU legislation.

Cyber Education and Training

Cyber specialists, decision-makers and users play a critical role against cyberattacks. Strengthening skills, education and awareness is thus key in building a cyber-resilient society. Pooling and sharing of training and exercises in order to create 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.

CYBER DEFENCE PILOT COURSES DEVELOPMENT SCHEME

Within this project, a methodology for developing Cyber Defence Training courses has been produced and is available for download on the EDA website. Further work packages in support of EDA Member States are the development of Cyber Pilot Courses:

- **Cyber Awareness Train-the-Trainer** – this course aims to build a network of EU and national cyber awareness trainers to improve interoperability. The pilot course is planned in cooperation with the European Security and Defence College (ESDC) from 26 – 28 October 2021 at the IT School of the Bundeswehr in Poecking, Germnay.

- **Cyber Implication for CSDP Military Crisis Action Planning** – the aim of this course is to develop a Cyber Operational Planning course for standardised preparation of Operational Planners of the EU and Member States in support of EU CSDP Operations, Missions and Exercises. The pilot course is planned in cooperation with the ESDC from 16 – 18 November 2021 in Brussels, Belgium.

- **Pilot Cyber and Hybrid Threats Course** – a pilot course on cyber and hybrid threats is currently under development. This course will educate participants about key elements of cyber defence and hybrid threats. Furthermore, it will provide students with individual training in order to enable them to address the implications of the intersection of cyber and hybrid. The execution of this course is planned for the first quarter 2022.

CYBER STRATEGIC DECISION-MAKING EXERCISES

The Cyber Strategic Decision-Making Exercises (SDM) train key governmental actors in Member States to face and manage an escalating cyber crisis in a hybrid context. The main objective is to promote awareness and improve understanding at political, administrative and military levels, supporting the strategic decision-making process, from a whole of government approach, considering relevant inputs from a cyber defence perspective and from a wider and comprehensive approach of hybrid threats. The SDM exercise has been developed by EDA since 2014, when the first pilot exercise was executed in Portugal. Since then, the SDMs were executed in different formats with Austria, Cyprus, the Czech Republic, Estonia, Greece, Latvia, and Slovenia.

CYBER PHALANX

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. CYBER PHALANX constitutes a compressed education and training opportunity while serving as an information and experience exchange platform. It is designed to be executed as a stand-alone exercise but it can also be integrated as a module in larger scale military exercises or elements like the course can also support a Work-Up of Staff (WUST) for headquarters. CYBER PHALANX was first executed in 2018 in Salzburg, Austria. The second iteration is planned from 27 September – 1 October 2021 in Lisbon, Portugal.

© LEONARDO

Cyber Defence Challenges in Air, Space, Maritime and Land

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

DEPLOYABLE CYBER EVIDENCE COLLECTION AND EVALUATION CAPABILITY (DCEC2)

Digital Forensics is a technology area that is well-established in the civilian context. Such technologies enable cybersecurity analysts to collect information and conduct investigations in response to cyber-attacks. On the military side, probably one of the tactical advantages that cyber forensics can provide is to help understanding adversaries' decision-making process and to reduce the time required for incident response. For the military context, cyber forensic exploitation teams must be enabled to work remotely or to deploy with forensic exploitation laboratories. Their functional operation must be scalable, modular, and agile to support a commander's needs, and must be configured in line with the operational infrastructure.

EDA is developing a DCEC2 technology demonstrator to provide deeper knowledge of state-of-the-art Digital Forensics applicable to CSDP.

AVIATION CYBER

EDA supports Member States to improve cybersecurity in the air domain. Advances in digitalisation and increased adoption of Information and Communication Technology are seen as a key enabler for the overall improvement of the Aviation System. These developments may for the time being, primarily consider civil aviation; however, they also have a significant impact on military aviation and civil/military coordination which is essential for the security of the airspace of each nation.

In addition, the challenges linked to the design, development, deployment and integration of networked equipment, new generations of manned and unmanned aerial platforms, the increased reliance on satellite-based PNT (Position, Navigation and Timing) aids, the modernisation of the CNS (Communication, Navigation and Surveillance) infrastructures and the exploitation of sensor fusion capabilities that rely on multiple data sources to create a degree of situational awareness not seen before, must be appropriately considered to ensure the highest possible degree of cyber resilience.

To support our Member States, EDA developed an ambitious work programme in 2017 through "The Military Aviation Cyber Engagement plan" which aims to follow a holistic approach in cybersecurity.

CYBERSECURITY IN THE DEFENCE SUPPLY CHAIN

This project focuses on creating a risk management model for military leaders with respect to cybersecurity risks posed to military capabilities by the supply chain and explore how these leaders might be supported by a web-based dashboard to improve situational awareness.

Cyber Defence Research and Technology

Member States must remain at the cutting edge of defence innovation and research. EDA supports the research into and the development of technologies essential to counter cybersecurity threats.

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

Participating Members: 🇩🇪 🇮🇹 🇪🇸

There is a need for capabilities to enable military commanders at all operational levels to understand and manage the risk of cyberattacks. The objective is 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 a CSDP context or any other framework. 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 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.

MULTI-AGENT SYSTEM FOR APT (ADVANCED PERSISTENT THREATS) DETECTION – MASFAD2

Participating Members: 🇧🇪 🇩🇪 🇳🇱

Existing, commercially available Off-The-Shelf (COTS) products experience difficulties in detecting advanced persistent attacks among the huge amount of network traffic generated from a multitude of network sources and military systems.

MASFAD 2 has been created in order to address these issues through the development of a next generation IDS (Intrusion Detection System) capable of monitoring distributed networks & detect APT (Advanced Persistent Threats).

Based on Machine Learning Algorithms & Log Aggregation/Correlation features MASFAD2 is capable of detecting previously unknown network threats.

Cyber related PESCO projects

The Permanent Structured Cooperation (PESCO) was established by a Council Decision on 11 December 2017, with 25 EU Member States. It offers a legal framework to jointly plan, develop and invest in shared capability projects, and enhance the operational readiness and contribution of armed forces. Currently (September 2021), four out of the 47 PESCO projects are cyber related.

CYBER RAPID RESPONSE TEAMS AND MUTUAL ASSISTANCE IN CYBER SECURITY (CRRT)

Coordinator: 🇱🇹 **Project Members:** 🇪🇪 🇭🇷 🇱🇹 🇳🇱 🇵🇱 🇷🇴

Cyber Rapid Response Teams (CRRTs) allow Member States to help each other to ensure a higher level of cyber resilience and collectively respond to cyber incidents. CRRTs could be used to assist other Member States, EU institutions, CSDP operations as well as partners. CRRTs are equipped with a commonly developed deployable cyber toolkits designed to detect, recognise and mitigate cyber threats. Teams are able to assist with training, vulnerability assessments and other requested support. Cyber Rapid Response Teams operate by pooling participating Member States experts. The CRRT PESCO project was successfully tested in the Dutch led Alarmex exerise in May 2021, demonstrating its operational capability.

CYBER THREATS & INCIDENT RESPONSE INFORMATION SHARING PLATFORM (CTIRISP)

Coordinator: 🇬🇷 **Project Members:** 🇨🇾 🇬🇷 🇪🇸 🇭🇺 🇮🇹 🇵🇹

The Cyber Threats and Incident Response Information Sharing Platform will develop more active defence measures, potentially moving from firewalls to more active measures. This project aims to help mitigate these risks by focusing on the sharing of cyber threat intelligence through a networked Member State platform, with the aim of strengthening national cyber defence capabilities.

CYBER AND INFORMATION DOMAIN COORDINATION CENTER (CIDCC)

Coordinator: 🇩🇪 **Project Members:** 🇫🇷 🇩🇪 🇭🇺 🇳🇱

The objective of the project is to develop, establish and operate a multinational Cyber and Information Domain (CID) Coordination Center (CIDCC) as a standing multinational military element, where – in line with the European resolution of 13 June 2018 on cyber defence – the participating Member States continuously contribute with national staff but decide sovereignly on case-by-case basis for which threat, incident and operation they contribute with means or information.

EU CYBER ACADEMIA AND INNOVATION HUB (EU CAIH)

Coordinator: 🇵🇹 **Project Members:** 🇵🇹 🇪🇸

To ensure a secure cyberspace, it is key to develop a technologically skilled workforce, a cyber-savvy ecosystem, and an effective pipeline of future employees. The project of EU CAIH can add value by enhancing the creation of an innovative web of knowledge for cyber defence and cybersecurity education and training, providing a vital contribution to strengthening national, NATO and EU's capability to defend against the threats of the digital world. It would also act as a coordination point for future cyber education, training and exercises, explore synergies with industry and academia, and establish an international cooperative approach, at the EU and NATO levels.

EUROPEAN
DEFENCE
AGENCY

European Defence Agency
Rue des Drapiers 17-23
B-1050 Brussels - Belgium

www.eda.europa.eu

Publications Office
of the European Union