EUROPEAN DEFENCE AGENCY

CYBER DEFENCE PROGRAM

Mario Beccia
Cyber Defence Program Manager

2019-09-17

Introduction

Part I: The Cyber Defence Strategic Context

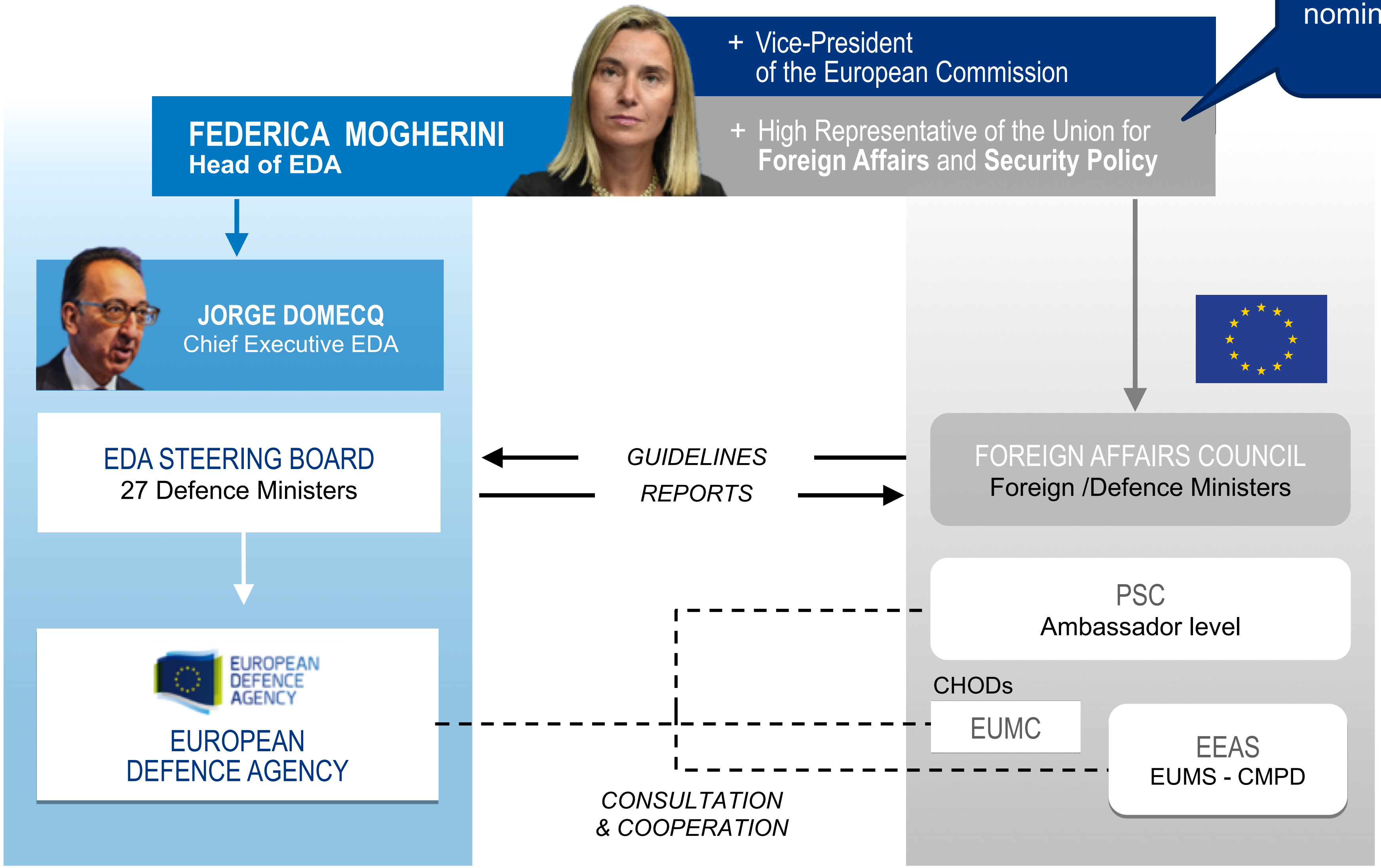
Part II: State of the Art

Part III: EDA Cyber Defence Program

INTRODUCTION

INSTITUTIONAL SETTING

Josep Borrell has been nominated has the next HR on Nov 2nd



FEDERICA MOGHERINI
Head of EDA

+ Vice-President of the European Commission

+ High Representative of the Union for **Foreign Affairs** and **Security Policy**

JORGE DOMECQ
Chief Executive EDA

EDA STEERING BOARD
27 Defence Ministers

EUROPEAN DEFENCE AGENCY

GUIDELINES

REPORTS

FOREIGN AFFAIRS COUNCIL
Foreign /Defence Ministers

PSC
Ambassador level

CHODs

EUMC

EEAS
EUMS - CMPD

CONSULTATION & COOPERATION

FACTS & FIGURES

Only EU Agency whose Steering Board meets at ministerial level

Established **2004**

Based in **BRUSSELS**

+-145 staff
connected with 2,500 experts in
Member States

Jorge Domecq
Chief Executive EDA

27 Member States
(all EU members except Denmark)
Administrative Arrangements
with Norway, Serbia, Switzerland and Ukraine

Budget 2018
€32.5 Mio

EDA Portfolio:
ca. 300 activities related to capability development, R&T and defence industry

Value R&T projects 2004-2017 run within EDA:
approx. €1 billion

MAIN MISSION

… to support the Council and the Member States in their effort to improve the Union's defence capabilities in the field of crisis management and to sustain the CSDP*

* Council decision 2015/1835
of 12 October 2015 on statute, seat and operational rules of the EDA

PART I – THE CYBER DEFENCE STRATEGIC CONTEXT

CYBERSPACE

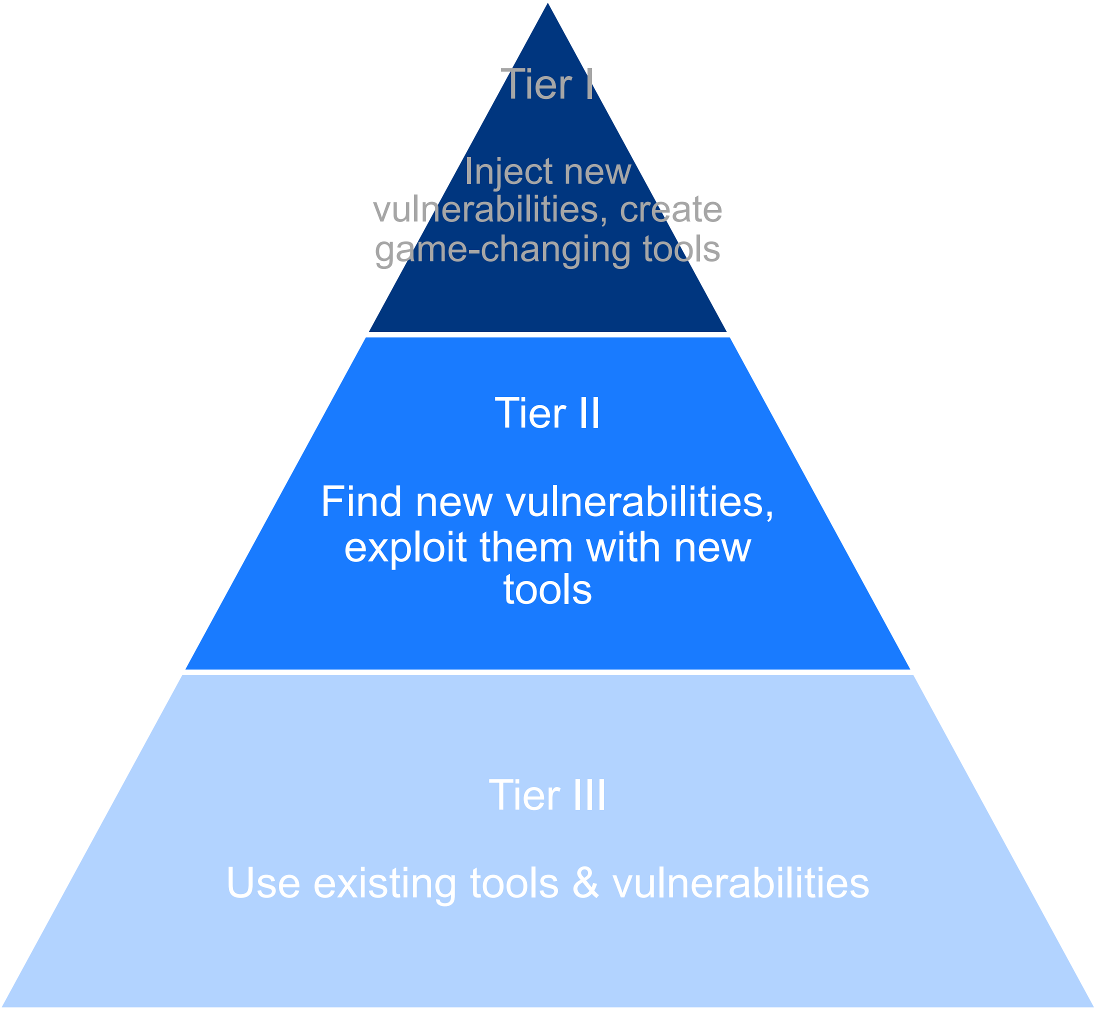
For the purpose of this session, cyberspace can be described with the following properties:

- Bilateral Human and network engagement
- Hyper connectivity and networking
- No geographical boundaries
- Not owned or controlled by governments, but by commercial entities

THREAT MODELING: STRIDE

- Spoofing
- Tampering
- Repudiation
- Information Disclosure
- Denial of service
- Elevation of priviledge

THREAT MODELING IN CYBERSPACE



Tier I

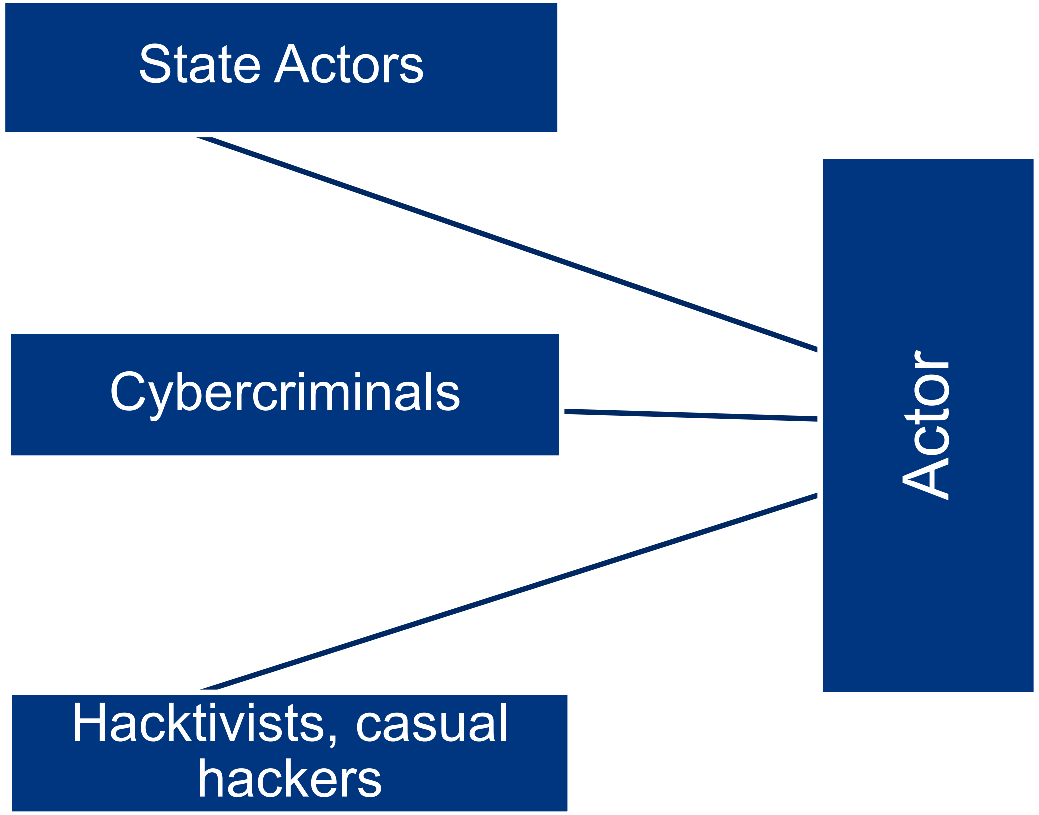
Inject new vulnerabilities, create game-changing tools

Tier II

Find new vulnerabilities, exploit them with new tools

Tier III

Use existing tools & vulnerabilities



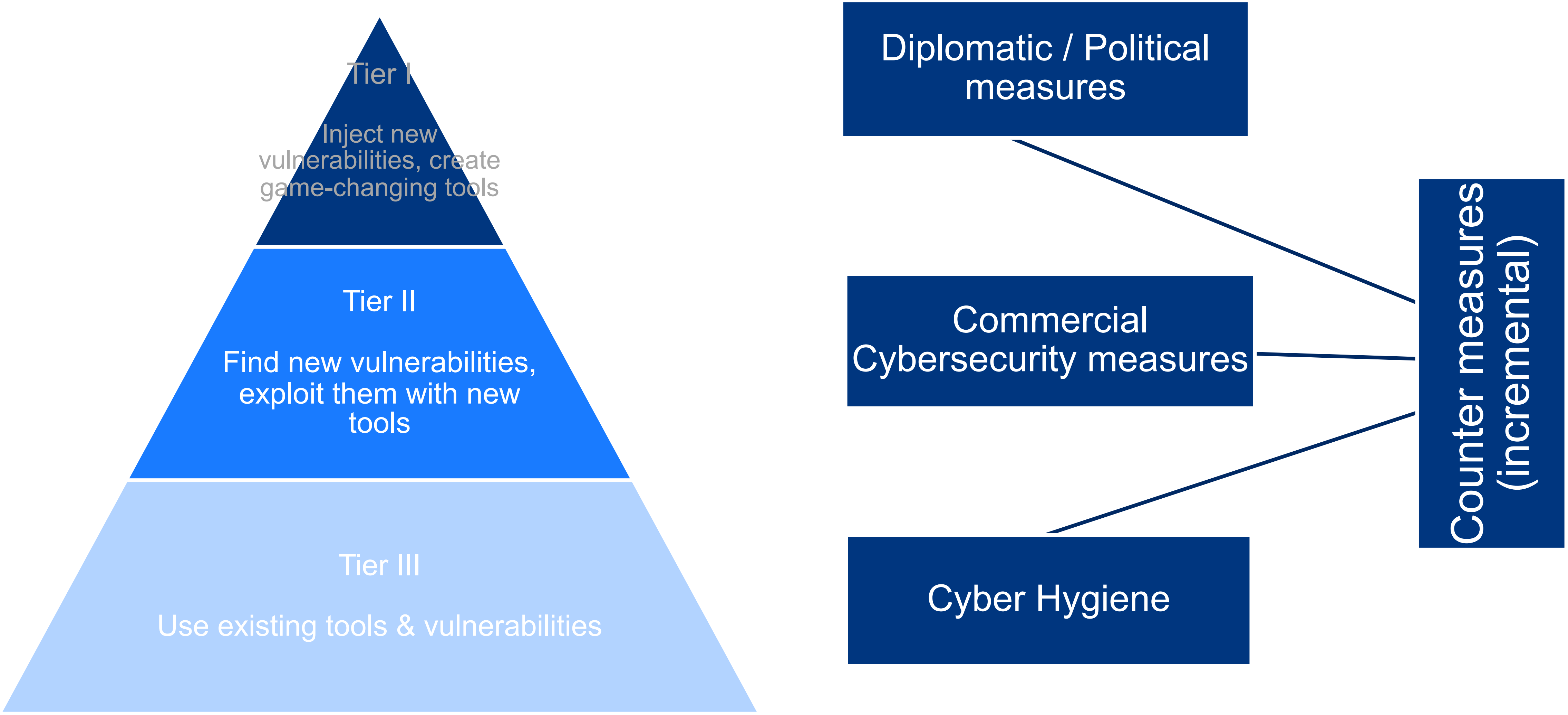
State Actors

Cybercriminals

Hacktivists, casual hackers

Actor

THREAT MODELING IN CYBERSPACE



Tier I

Inject new vulnerabilities, create game-changing tools

Tier II

Find new vulnerabilities, exploit them with new tools

Tier III

Use existing tools & vulnerabilities

Diplomatic / Political measures

Commercial Cybersecurity measures

Cyber Hygiene

Counter measures (incremental)

WHAT’S OUR MISSION IN CYBERSPACE?

Achieve Better Cybersecurity Resilience

“BETTER”

Just like “security”*, Cybersecurity is a “*relative state*” that should be aimed at, but can never be fully achieved

** Security is “the quality or state of being secure”, Merriam-Webster dictionary (https://www.merriam-webster.com/dictionary/security)*

CYBERSECURITY

- Oxford dictionary

  *“The **state** of being protected against the criminal or unauthorized use of electronic data, or the measures taken to achieve this”*

- ISO/IEC 27032:2012

  “Preservation of confidentiality, integrity and availability of information in the Cyberspace”

RESILIENCE

- **ISO/IEC 22316**

  “The ability of an organization to absorb and adapt in a changing environment”

- Principles:
  - The behaviors of all members of an organization need to contribute to organizational resilience
  - Diversity of skills is very important, as new threats, challenges, and opportunities may originate from different areas within the organization or from its environment
- Attributes
  - Understanding the context of the organization
  - Continual improvement

CYBER RESILIENCE

Cyber Resilience = *Cyber*security + Business *Resilience*[*]

- Risk **Management**, as opposed to Risk **Avoidance**
- **Manage the “unknown”** (known and unknown unknowns), as opposed to manage the “known”
- People, Process, Technology

Source: adapted from the ISO27001 definition of Cyber Resilience

CYBER RESILIENCE: GOALS

- **Anticipate** → *Maintain* a state of informed preparedness in order to forestall compromises of mission/business functions from adversary attacks

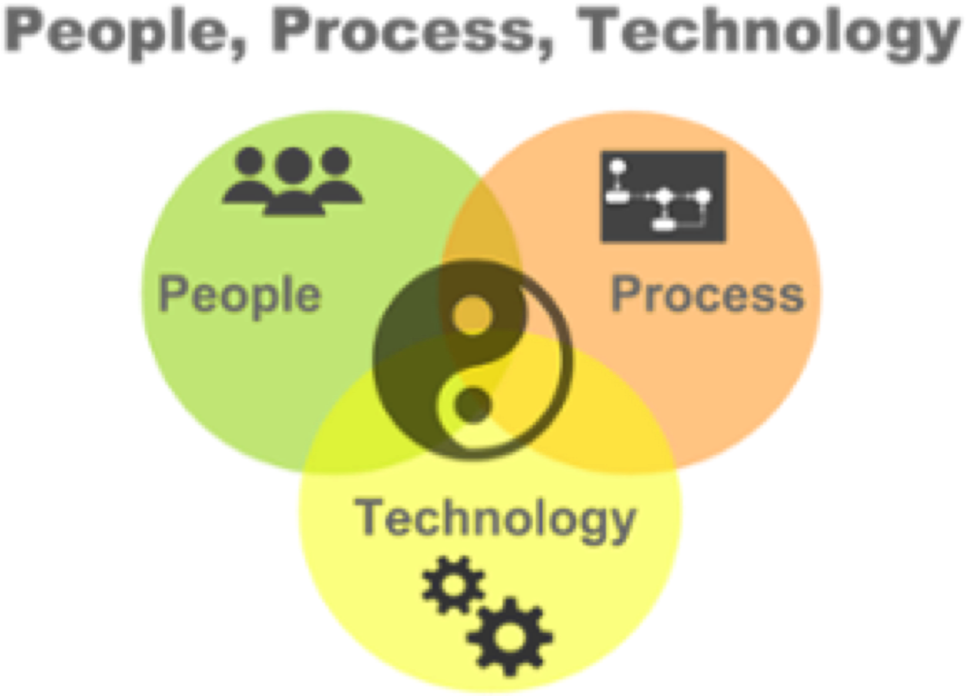
- **Withstand** → *Continue* essential mission/business functions despite successful execution of an attack by an adversary

- **Recover** → *Restore* mission/business functions to the maximum extent possible subsequent to successful execution of an attack by an adversary

- **Evolve** → *To change* missions/business functions, so as to minimize adverse impacts from actual or predicted adversary attacks

ACHIEVE BETTER CYBERSECURITY RESILIENCE

- Better cybersecurity resilience implies:
  - Better preparedness (people)
  - Better organization of assets (process)
  - Better assets (technology)
- A mixture of cybersecurity capabilities (in the DOTMLPFI sense, including materiel, personnel, organization, etc…)
- Once in place, appropriate capabilities ensure the ability to execute processes across the entire scope of cybersecurity, such as:
  - Preparedness
  - Incident analysis and response
  - Deterrence
  - Information sharing



PART II – STATE OF THE ART

THE CYBER DEFENCE LANDSCAPING STUDY

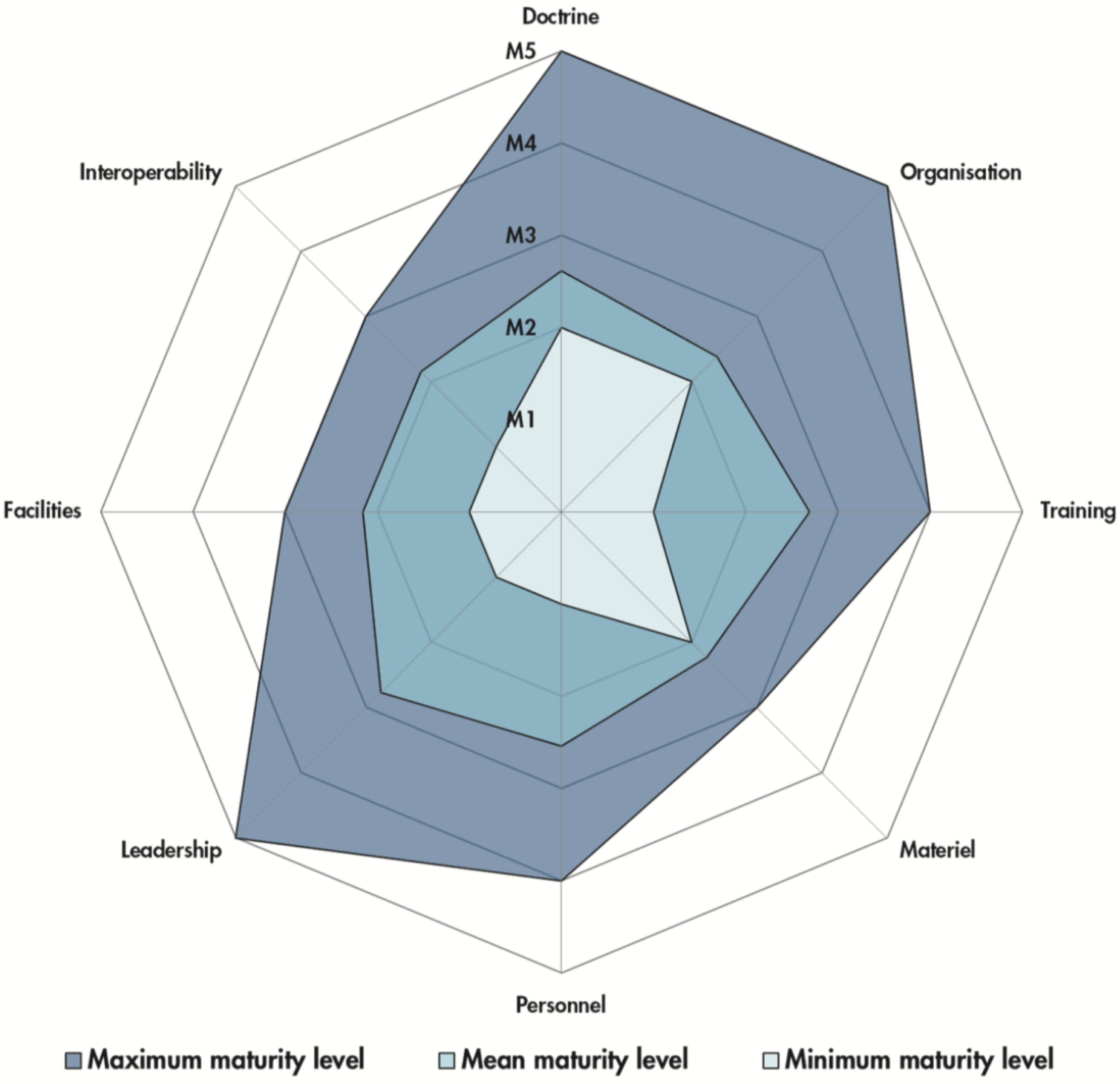
- A number of initiatives are taken to analyze and understand MS initiative and “state-of-the-art” of Cyber Defence in each MS
- In 2012, a first round of landscaping was performed
- In 2018, a new round was completed, and supported the creation of the Cyber Defence area of the CDP (13 MS responded to the study providing details on their capdev programs)
- The objective of the landscaping study can be described as follows:

Provide a holistic, multi-dimensional, mid-to-long term perspective of European cyber defence capabilities, augmenting the EU Cyber Defence Policy Framework reporting and the CDP 2018 with a comprehensive and full spectrum view of cyber defence capabilities

OVERALL MATURITY

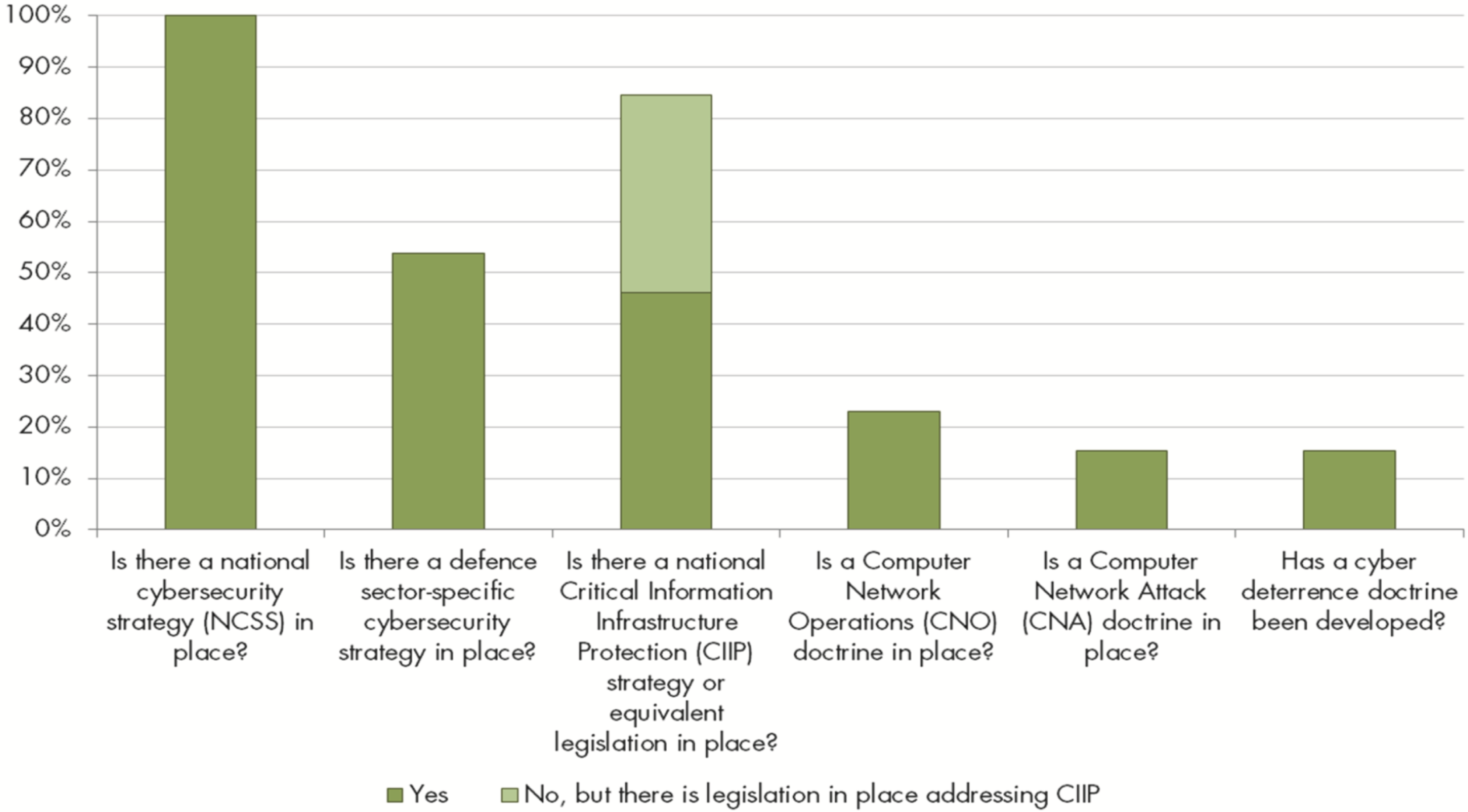
On average pMS are **located between emerging (M2) and established (M3) levels of maturity** across all pillars

- Doctrine, Training and Leadership are those where pMS perform better on average
- Across most DLODs different, individual pMS display an advanced(M4) or Forward Looking (M5) level of maturity
- No MS reported a maturity level below M2 (Emerging) for Doctrine, Organisation and Materiel

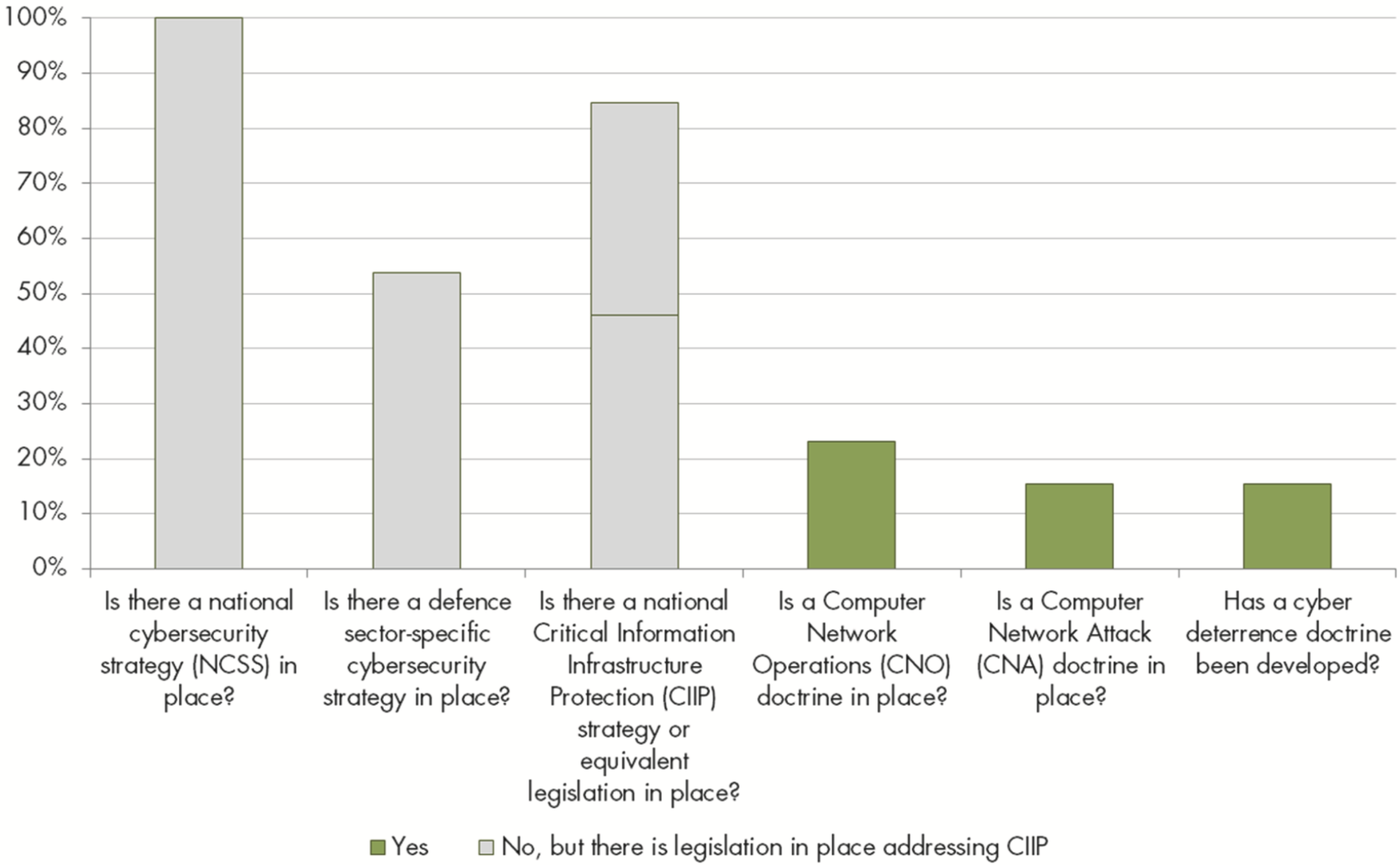


EUROPEAN DEFENCE AGENCY

2018: ESSENTIAL PROVISIONS

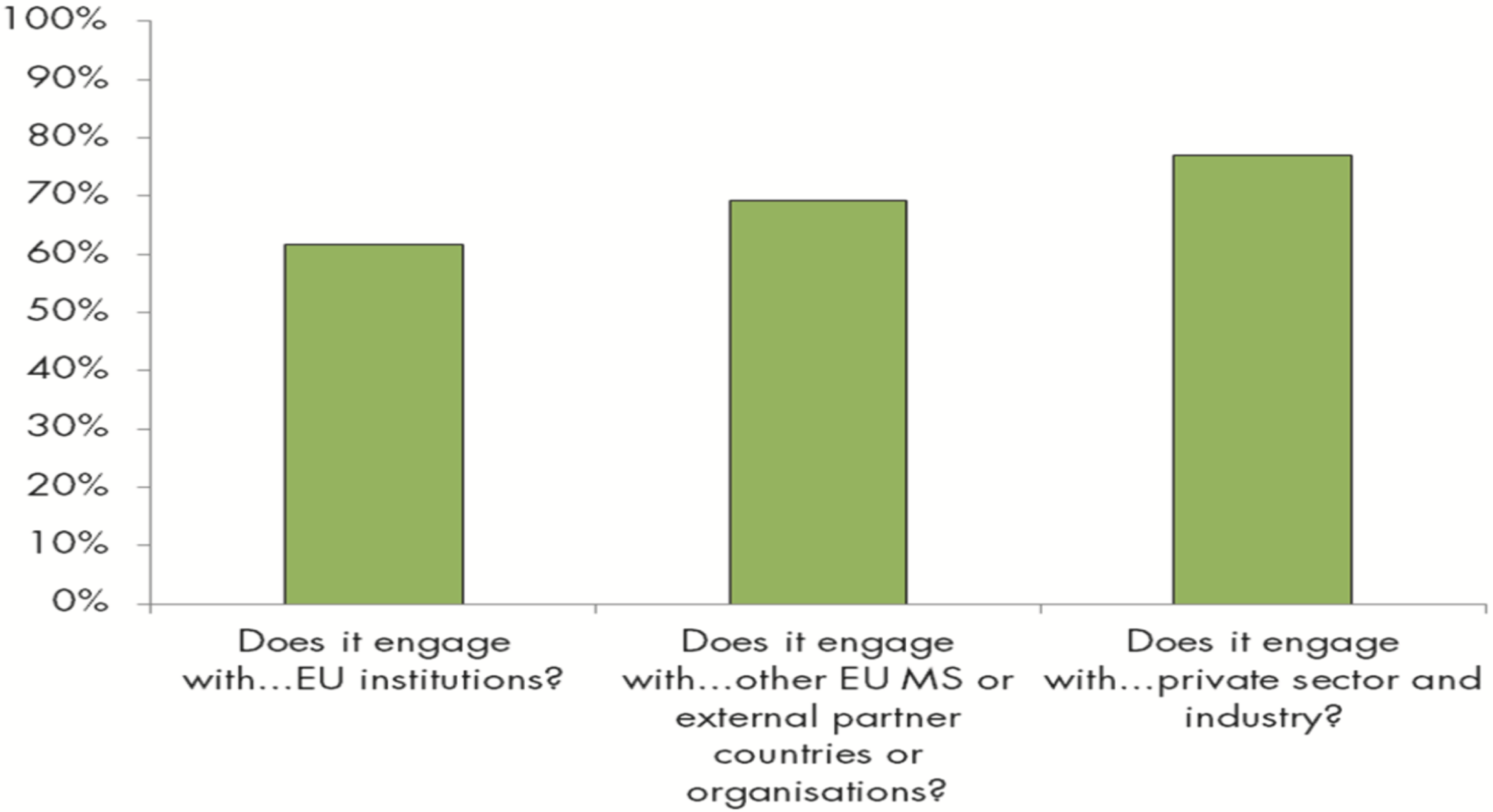


A DEVELOPING STRATEGIC APPROACH



A DEDICATED ENTITY

- All MSs have established a strategic national level cybersecurity steering group or committee
- There appears to be margin for improvement as regards regular collaboration between national strategic committees and other stakeholders



PART III – EDA CYBER DEFENCE PROGRAM

CAPABILITY DEVELOPMENT PLAN (CDP)

OBJECTIVE

Provide Member States with comprehensive picture of European capability requirements over time

CDP REVISION

- New set of CDP priorities to be approved by July 2018
- Capability driven, R&T and industry dimension included

KEY FEATURES

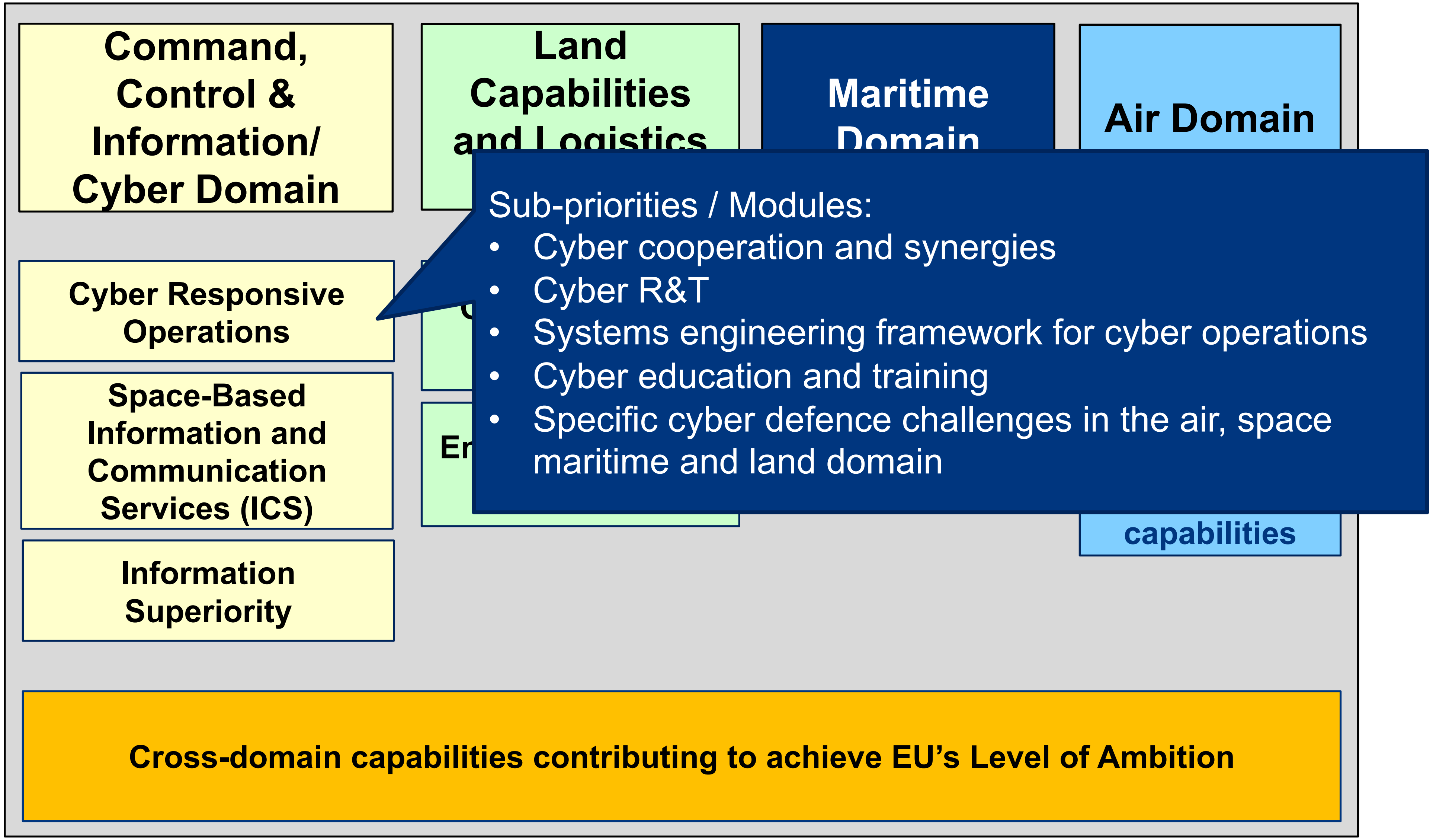
- Output-oriented
- Coherence with NATO Defence Planning Process, National Plans & Programmes
- Implications of new security challenges (EUGS) incl. hybrid threats included

EDA ROLE

EDA is the architect of the CDP and as such:

Works with experts from Member States, EU bodies and industry on consolidating information on short-, mid- and long-term capability needs

2018 EU CAPABILITY DEVELOPMENT PRIORITIES



Command, Control & Information/ Cyber Domain

Land Capabilities and Logistics

Maritime Domain

Air Domain

Cyber Responsive Operations

Space-Based Information and Communication Services (ICS)

Information Superiority

C

En

capabilities

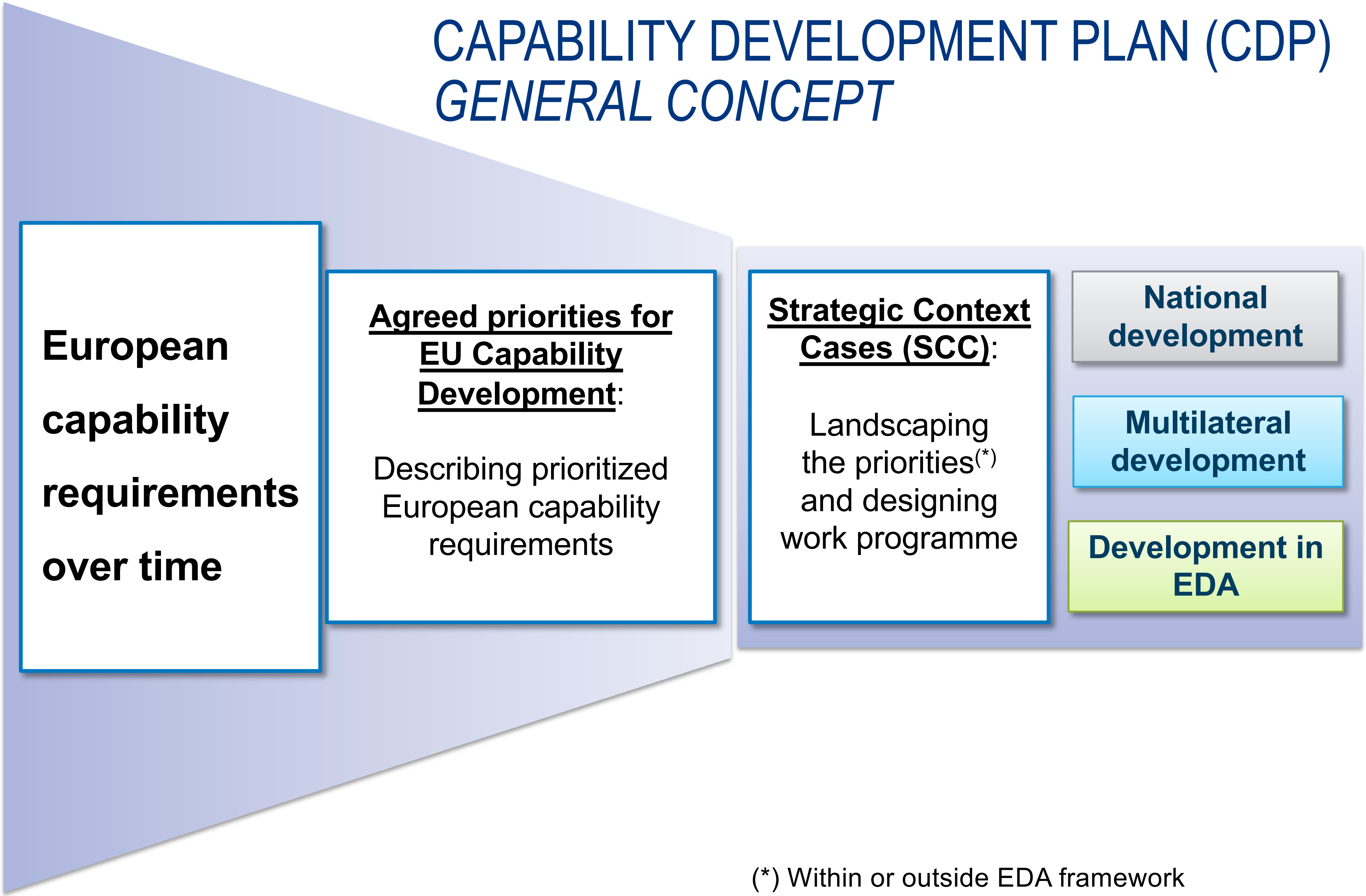
Sub-priorities / Modules:

- Cyber cooperation and synergies
- Cyber R&T
- Systems engineering framework for cyber operations
- Cyber education and training
- Specific cyber defence challenges in the air, space maritime and land domain

Cross-domain capabilities contributing to achieve EU's Level of Ambition

CAPABILITY DEVELOPMENT PLAN (CDP)

GENERAL CONCEPT



European capability requirements over time

Agreed priorities for EU Capability Development:

Describing prioritized European capability requirements

Strategic Context Cases (SCC):

Landscaping the priorities(*) and designing work programme

National development

Multilateral development

Development in EDA

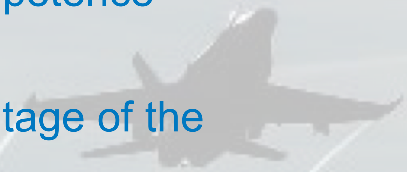
(*) Within or outside EDA framework

CHALLENGES (SHORT TERM)

- To synchronize efforts between EU agencies and other entities active in the Cyber domain within existing policy frameworks (MoU; EU/NATO Joint Declaration)
- To improve the collaboration between Member States in R&T activities, with specific attention to urgent R&T needs and to establishing a common and systematic approach;
- To develop a common framework in support of systems engineering;
- To establish a more coherent approach to military training & education in the cyber domain;
- To increase awareness and understanding of cyber defence challenges in the Air Land, Maritime and Space domains;

EDA SUPPORT ACTIONS

- Foster existing cooperation and identify further areas for cooperation (such as with NATO ACT, CCD CoE, NCIA, ESCD; ESA; EUROPOL, ENISA, CERT-EU; ECSO, ASD; Academia; EU initiatives such as Network of Cybersecurity Competence Centers)
- Facilitate the launch of cooperative initiatives at EU level taking advantage of the Cyber Technology Landscaping results
- Stimulate and promote the development of an EU industrial base for Cyber Defence capabilities, also by encouraging Research and Technology in the field along a standardized and interoperable systems engineering approach;
- Support the harmonization of requirements for Cyber Defence capabilities across pMS;
- Promote the creation and sustainment of an effective and efficient military workforce in the Cyber Domain, in support of CSDP and pMS' organizations;
- Promote and sustain a review of existing military CD training systems and capabilities to assess and evolve their Cyber Defence posture
- Identify further challenges in other military domains that have Cyber implications;
- Stimulate and promote the development of an EU industrial base for Cyber Defence capabilities, also by encouraging Research and Technology in the field;
- Support the creation of modern policies in support of supply chain security and modernization



CYBER DEFENCE PROJECTS AND INITIATIVES

Ad-hoc projects

- Cyber Ranges Federation
- CySAP (Cyber Defence Situation Awareness)
- DCEC2 (Deployable Forensics)

Training & Education

- CYBRID / Cyber Defence for EU Institutions
- Senior Decision Makers Seminar
- Operational Cyber Defence / Cyber Phalanx

Support to PESCO projects

- "Cooperative Rapid Response Teams for Cyber Defence", LT led
- "Cyber Threats and Incident Response Information Sharing Platform", EL led

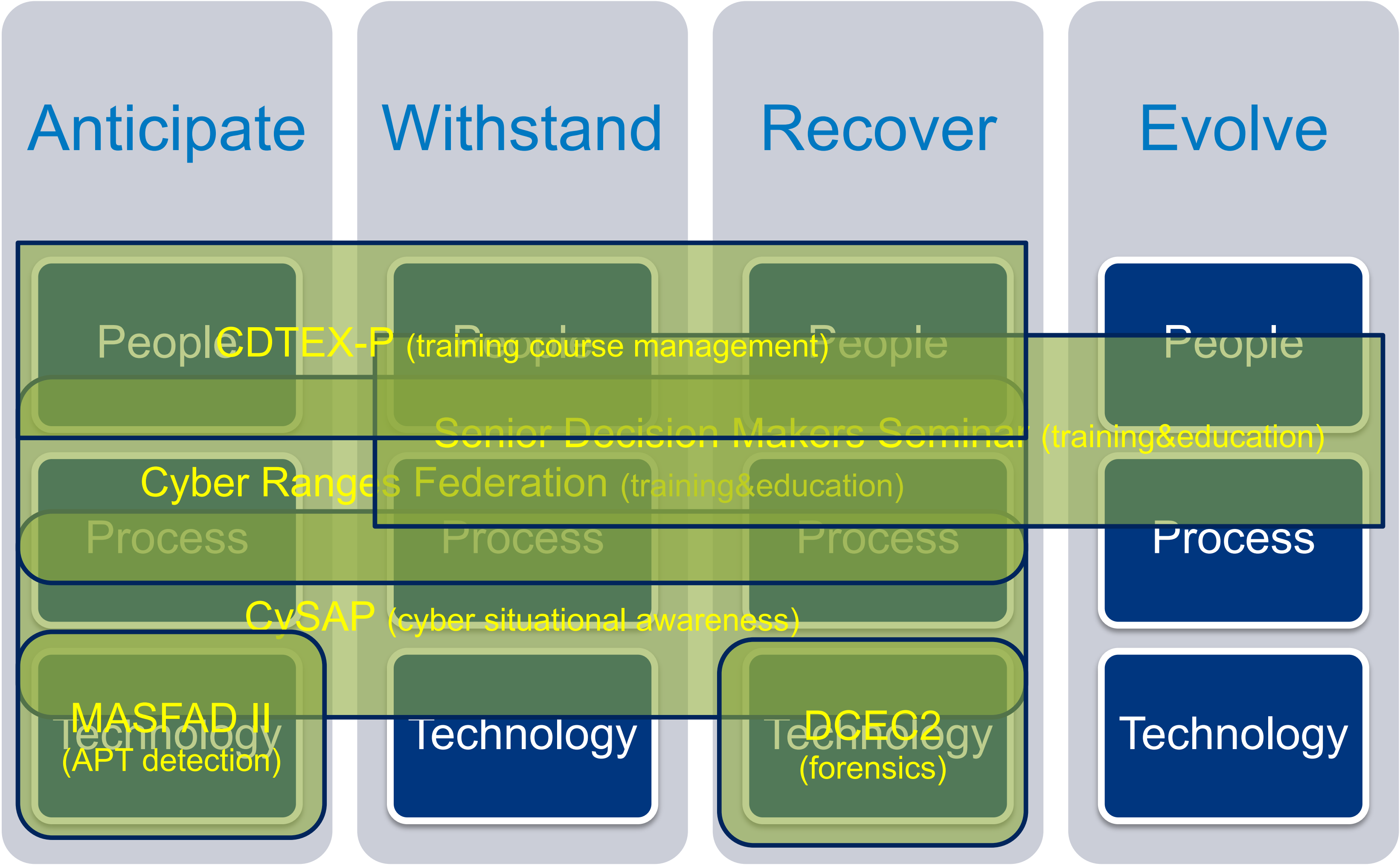
Teams and other initiatives

- Project Team Cyber Defence
  - Meets 3 times per year
  - All EU MSs formally participating, 16 to 20 attending each meeting
- Cyber Defence Ad Hoc Working Group
- Specialized workshops

Policy and Cooperation

- Support the evolution and adaptation of the Cyber Defence Policy Framework
- Enhance cooperation with other EU Institutions and third parties (NATO)
- support the implementation of the CSDP

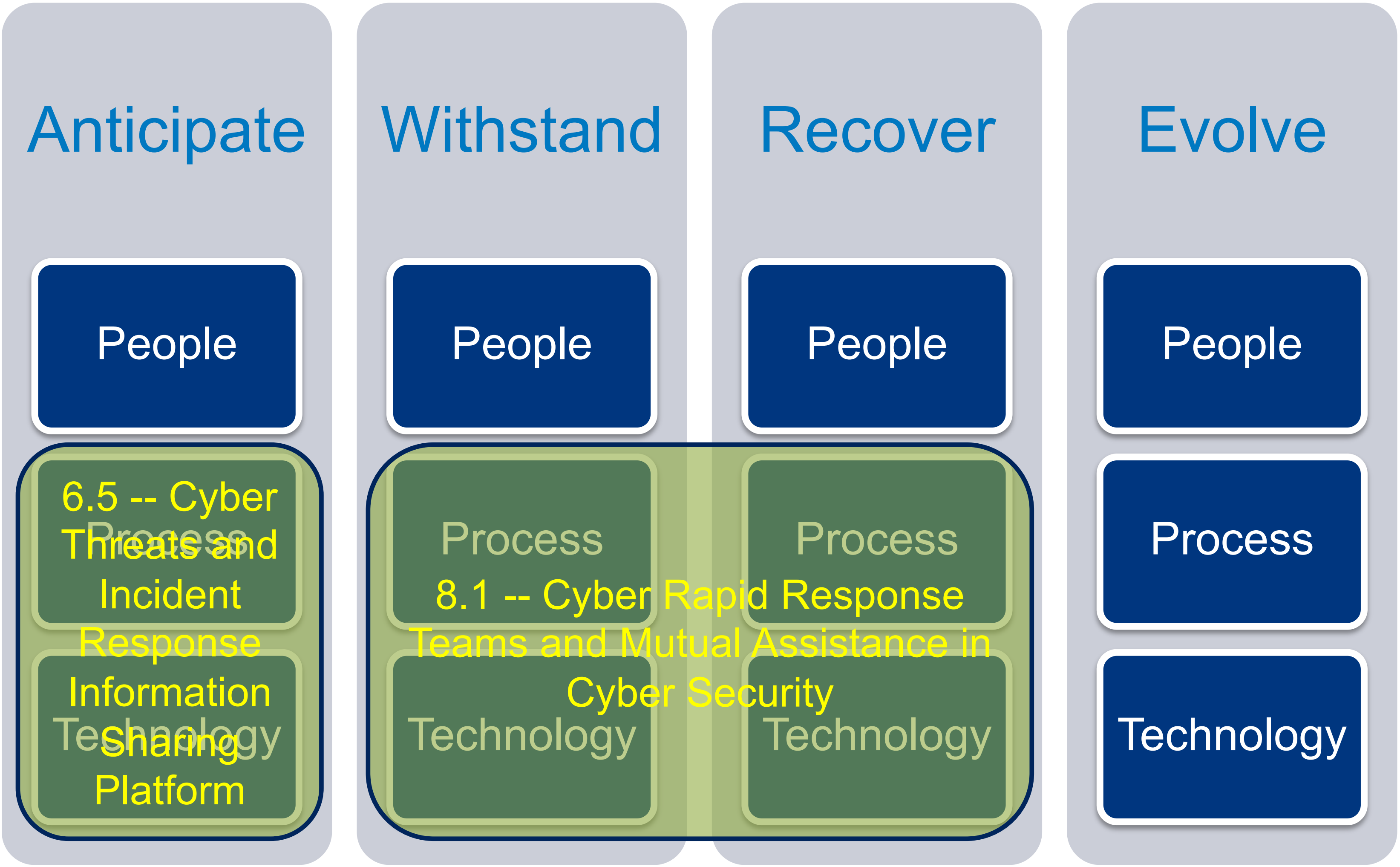
EDA ACTIVE PROJECTS



Anticipate
Withstand
Recover
Evolve
People
People
People
People
Process
Process
Process
Process
Technology
Technology
Technology
Technology
CDTEX-P (training course management)
Senior Decision Makers Seminar (training&education)
Cyber Ranges Federation (training&education)
CySAP (cyber situational awareness)
MASFAD II
(APT detection)
DCEO2
(forensics)

EUROPEAN DEFENCE AGENCY

PESCO PROJECTS FOR CYBER DEFENCE



Anticipate

People

Process

Technology

6.5 -- Cyber Threats and Incident Response Information Sharing Platform

Withstand

People

Process

Technology

Recover

People

Process

Technology

8.1 -- Cyber Rapid Response Teams and Mutual Assistance in Cyber Security

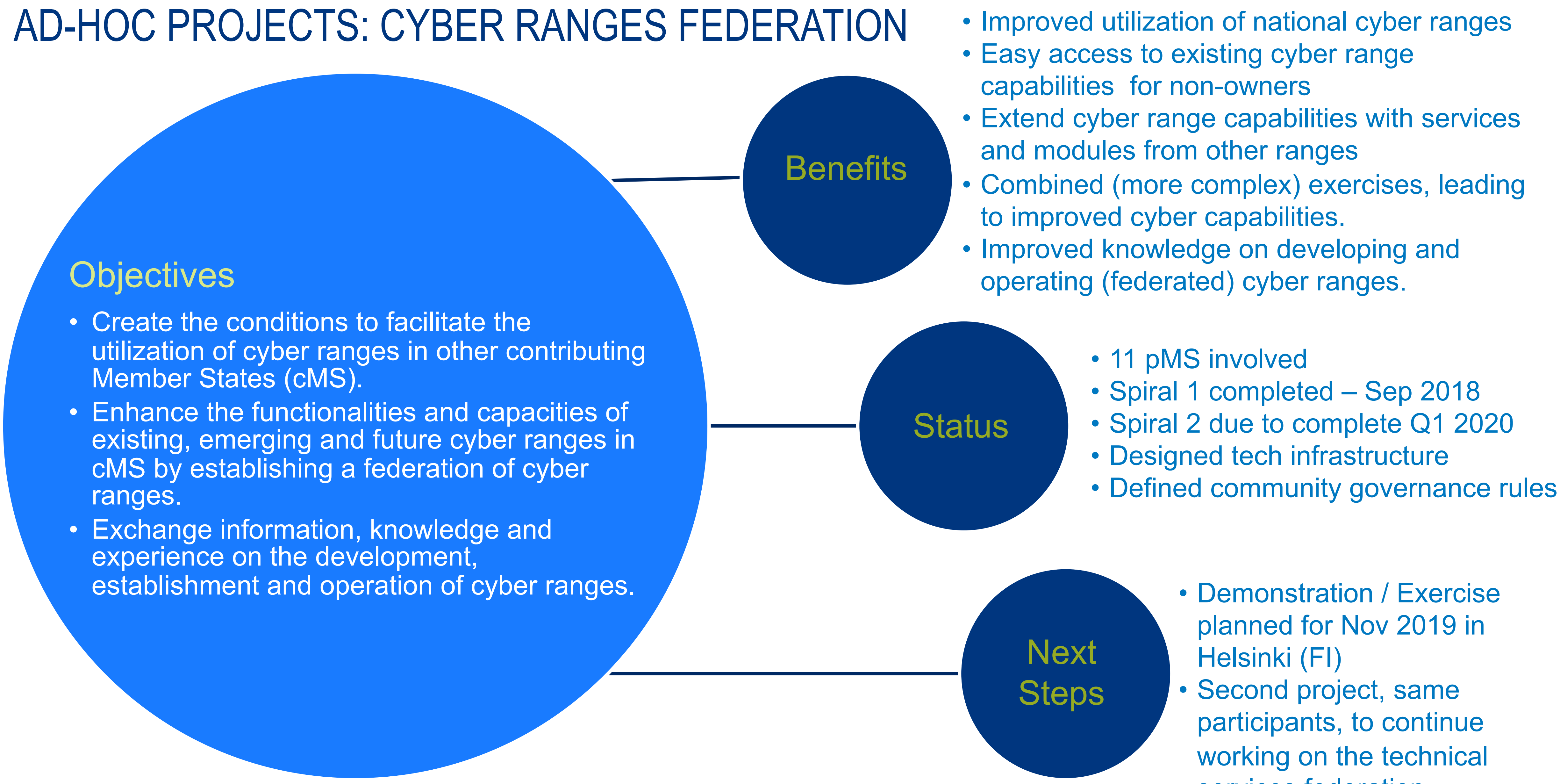
Evolve

People

Process

Technology

AD-HOC PROJECTS: CYBER RANGES FEDERATION



Objectives

- Create the conditions to facilitate the utilization of cyber ranges in other contributing Member States (cMS).
- Enhance the functionalities and capacities of existing, emerging and future cyber ranges in cMS by establishing a federation of cyber ranges.
- Exchange information, knowledge and experience on the development, establishment and operation of cyber ranges.

Benefits

- Improved utilization of national cyber ranges
- Easy access to existing cyber range capabilities for non-owners
- Extend cyber range capabilities with services and modules from other ranges
- Combined (more complex) exercises, leading to improved cyber capabilities.
- Improved knowledge on developing and operating (federated) cyber ranges.

Status

- 11 pMS involved
- Spiral 1 completed – Sep 2018
- Spiral 2 due to complete Q1 2020
- Designed tech infrastructure
- Defined community governance rules

Next Steps

- Demonstration / Exercise planned for Nov 2019 in Helsinki (FI)
- Second project, same participants, to continue working on the technical services federation

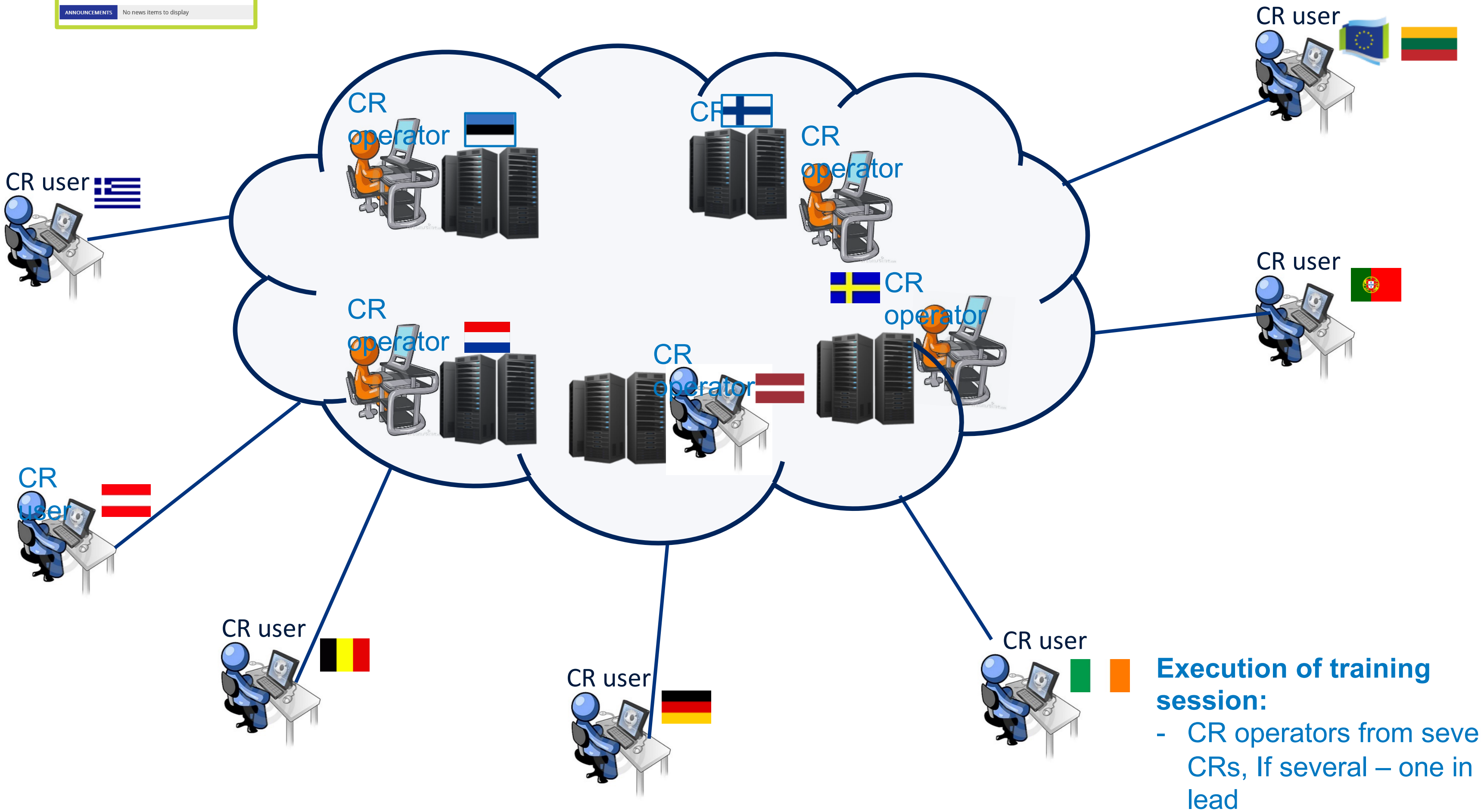
AD-HOC PROJECTS: CYBER RANGES FEDERATION ENVISIONED END-STATE

Planning of training session:

- CR availability and CR services through CDTEXP according to the Service catalogue
- CR owner contact information
- Basics to arrange exercise using federation

EUROPEAN DEFENCE AGENCY CD TEXP

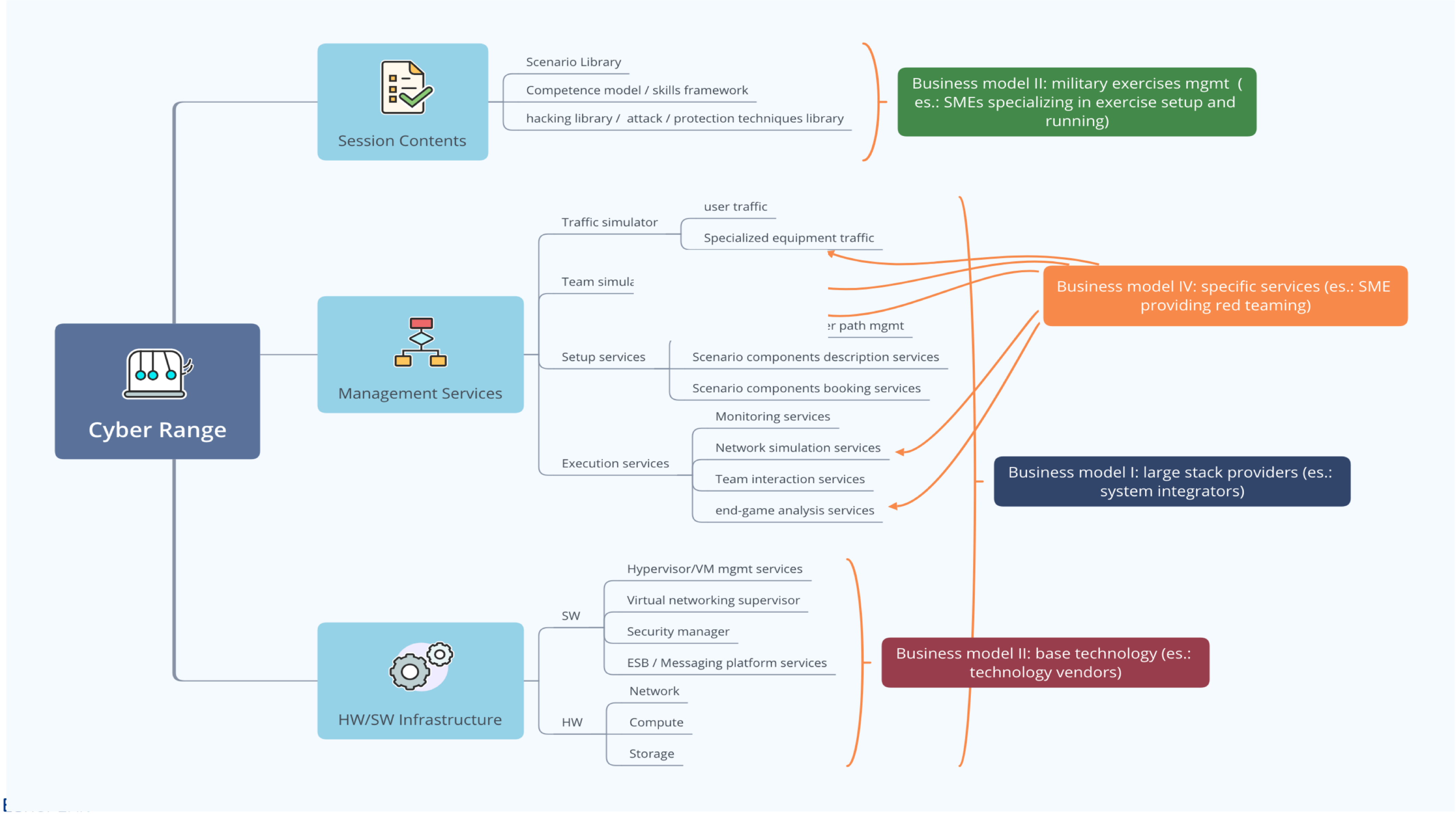
ANNOUNCEMENTS No news items to display



Execution of training session:

- CR operators from several CRs, If several – one in lead
- Existing services and scenarios from cMS

CYBER RANGES FEDERATION – ARCHITECTURE AND BUSINESS MODELS



Cyber Range

Session Contents

Scenario Library

Competence model / skills framework

hacking library / attack / protection techniques library

Business model II: military exercises mgmt (es.: SMEs specializing in exercise setup and running)

Management Services

Traffic simulator

user traffic

Specialized equipment traffic

Team simula

r path mgmt

Setup services

Scenario components description services

Scenario components booking services

Execution services

Monitoring services

Network simulation services

Team interaction services

end-game analysis services

Business model IV: specific services (es.: SME providing red teaming)

Business model I: large stack providers (es.: system integrators)

HW/SW Infrastructure

SW

Hypervisor/VM mgmt services

Virtual networking supervisor

Security manager

ESB / Messaging platform services

HW

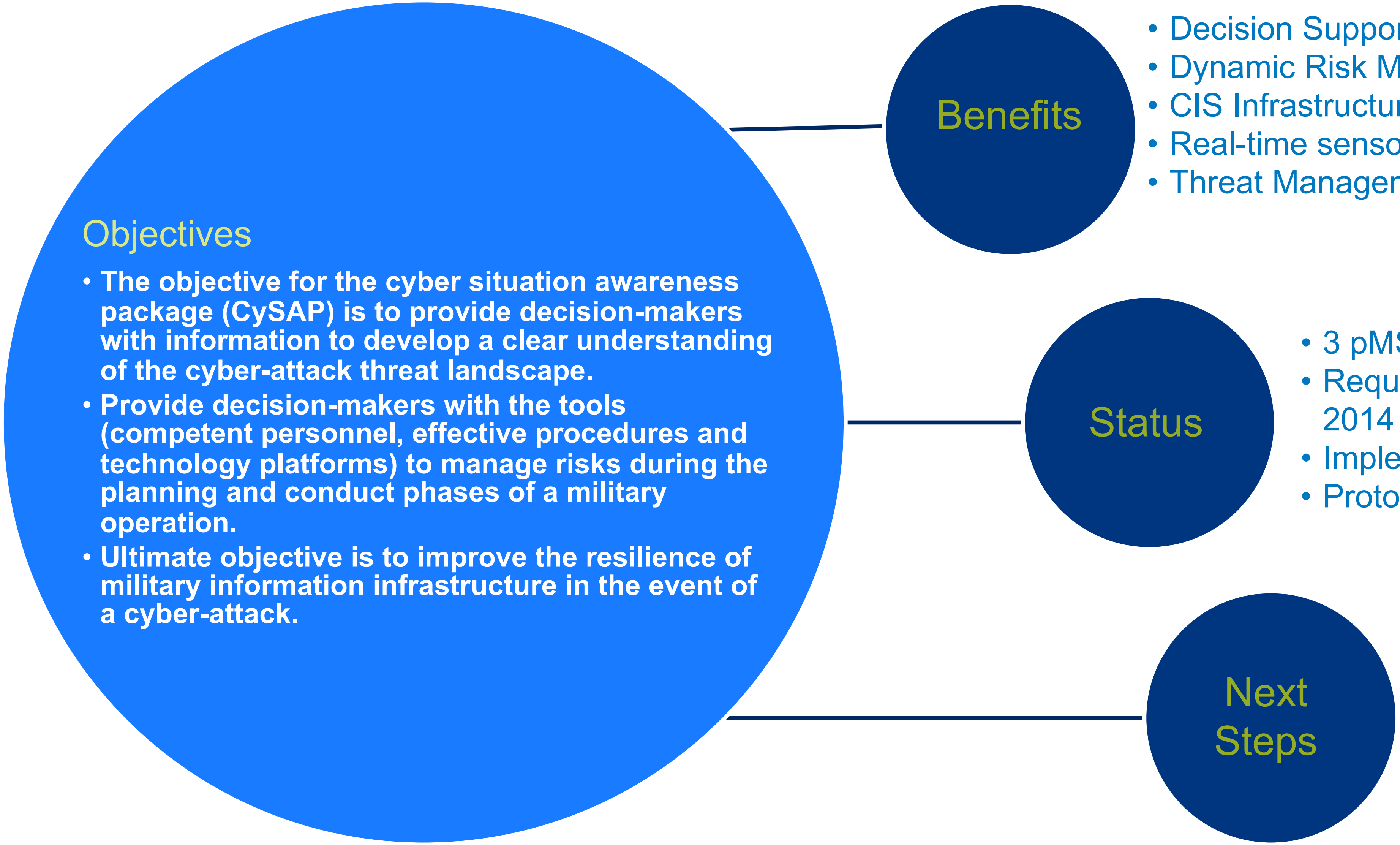
Network

Compute

Storage

Business model II: base technology (es.: technology vendors)

AD-HOC PROJECTS: CYSAP



Objectives

- **The objective for the cyber situation awareness package (CySAP) is to provide decision-makers with information to develop a clear understanding of the cyber-attack threat landscape.**
- **Provide decision-makers with the tools (competent personnel, effective procedures and technology platforms) to manage risks during the planning and conduct phases of a military operation.**
- **Ultimate objective is to improve the resilience of military information infrastructure in the event of a cyber-attack.**

Benefits

- Decision Support
- Dynamic Risk Management
- CIS Infrastructure discovery
- Real-time sensor interface
- Threat Management

Status

- 3 pMS involved
- Requirements definition between 2014 and 2018
- Implementation kickoff in Jan 2019
- Prototype expected by Q2 2020

Next Steps

- Validation of the technical architecture design
- Validation of prototype architecture

OB PROJECT: DEPLOYABLE CYBER EVIDENCE COLLECTION AND EVALUATION CAPACITY (DCEC2)

Objectives

- Deliver a deployable forensics technology demonstrator for military operations.
- Perform an analysis of the state-of-the-art of digital forensics science, technology and practice will be performed, looking for a functional relevance to the defence sector.
- Identify technology trends and solutions in a roadmap, including anti-forensics measures and examination of future technologies

Benefits

- Deployable forensics prototype for evaluation
- Definition of processes and technologies for state-of-the-art of deployable forensics
- Validation of processes and technologies in military exercises

Status

- 2 pMS involved
- Requirements definition between 2016 and 2018
- First prototype delivered in Q4 2018
- Conversion from EDA initiative into AdHoc project expected by end of 2019

Next Steps

- Validation of prototype
- AdHoc project converstion

CYBER DEFENCE EXERCISE FORMATS UNDER DEVELOPMENT

EU CYBRID

- EU Defence Ministers, EEAS, ENISA, EE MoD in cooperation with EDA during EE Council Presidency
- Simulated attack on the EU’s military structures
- “various technical problems could quickly develop into questions requiring political guidance”

Senior Decision Maker Seminar (SDM)

- Government level
- Involving decision-making bodies of a nation + private sector
- Separation into "standardised" teams, e.g. military & intelligence, justice, private sector

Operational Cyber Defence

- Military operational planners
- Multiple nations involved
- Complex military mission scenario in a cyber – contested environment

Last words…

…thank you!

FOR MORE INFORMATION
WWW.EDA.EUROPA.EU

FOLLOW US ON TWITTER
@EUDEFENCEAGENCY

EUROPEAN
DEFENCE
AGENCY