



AI AND CYBER DEFENCE

6 APPLICATIONS, 1 CHALLENGE

Mr. Mario Beccia
Program Manager Cyber Defence





ABOUT EDA

FACTS & FIGURES

Only EU Agency whose Steering Board meets at ministerial level



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

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

CDP and the Cyber Domain

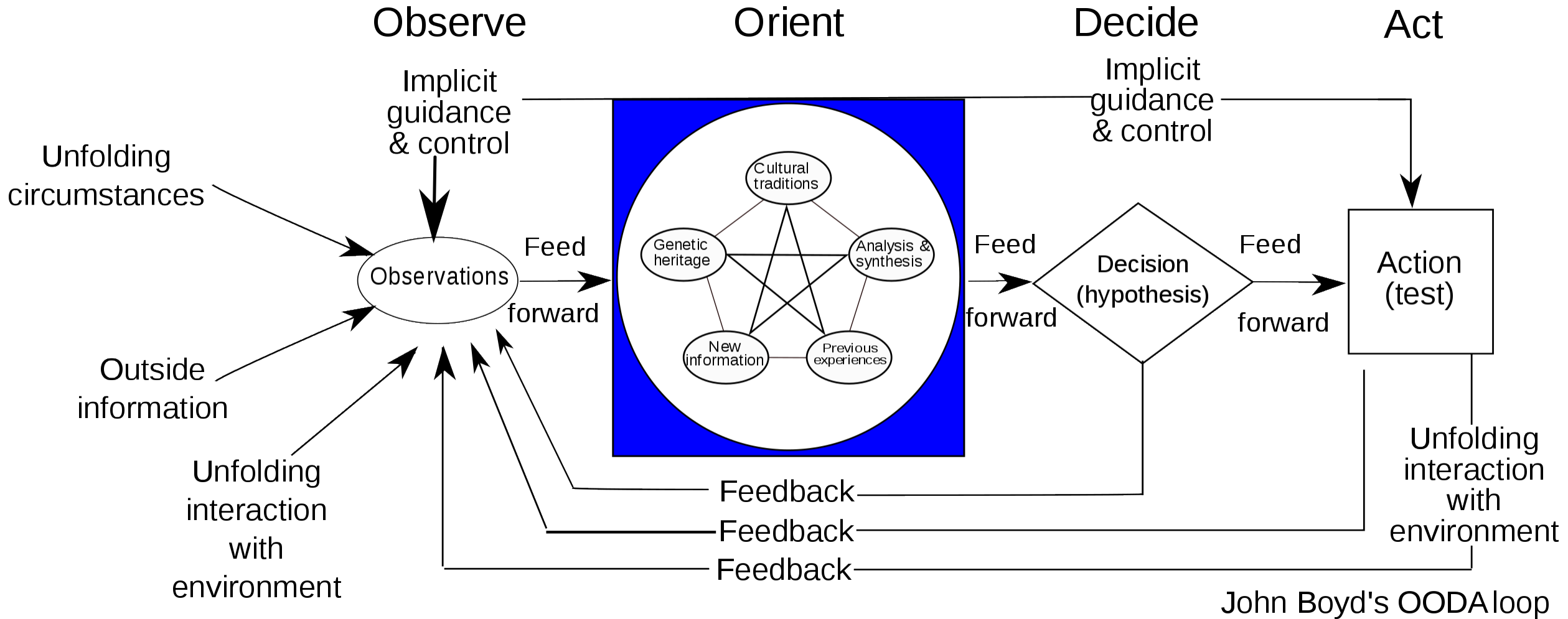
PRIORITY: ENABLING CAPABILITIES FOR CYBER RESPONSIVE OPERATIONS

- >> 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

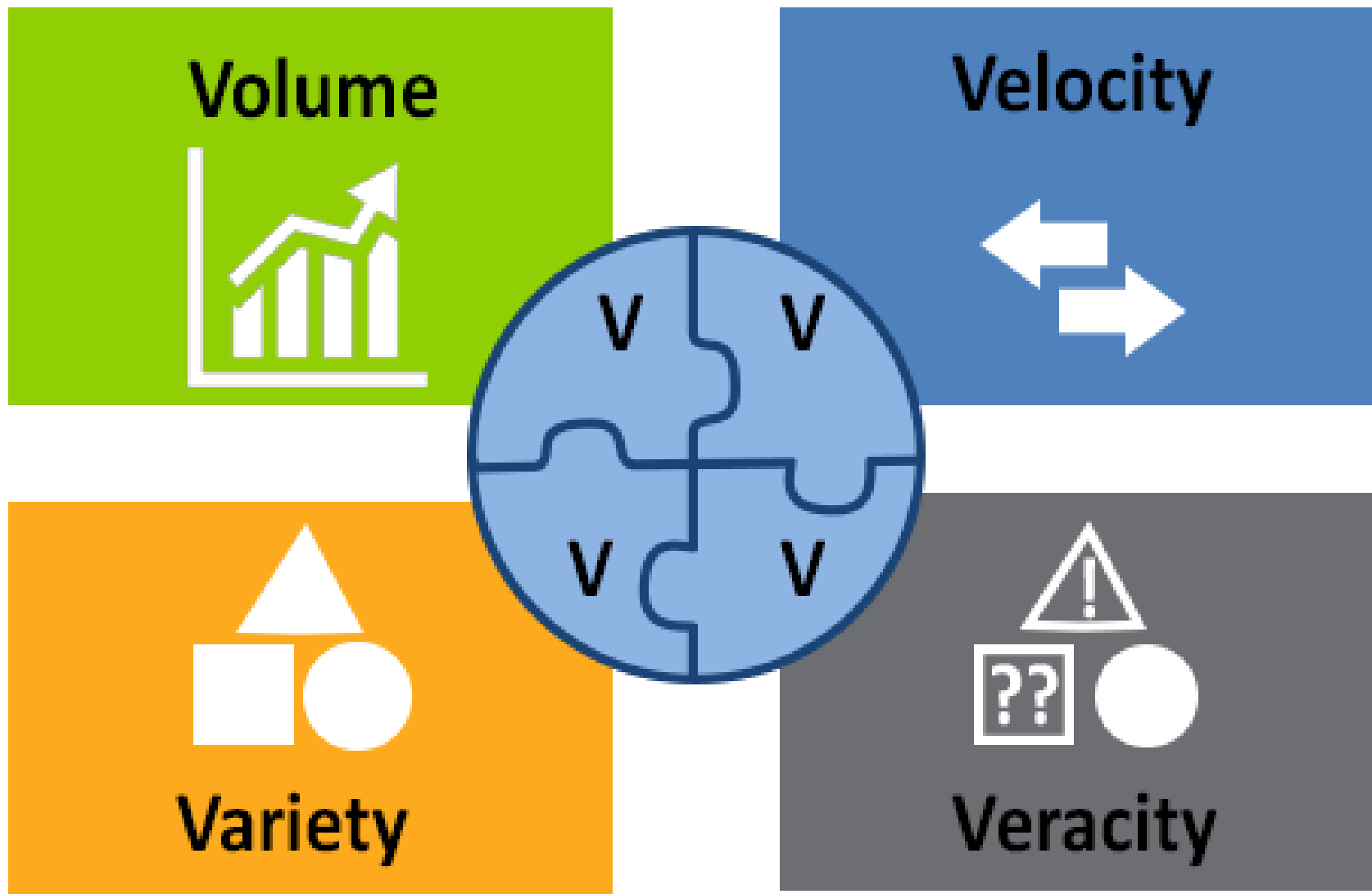


AI AND CYBER DEFENCE

DECISION-MAKING (THE OODA LOOP)



CHALLENGES/I



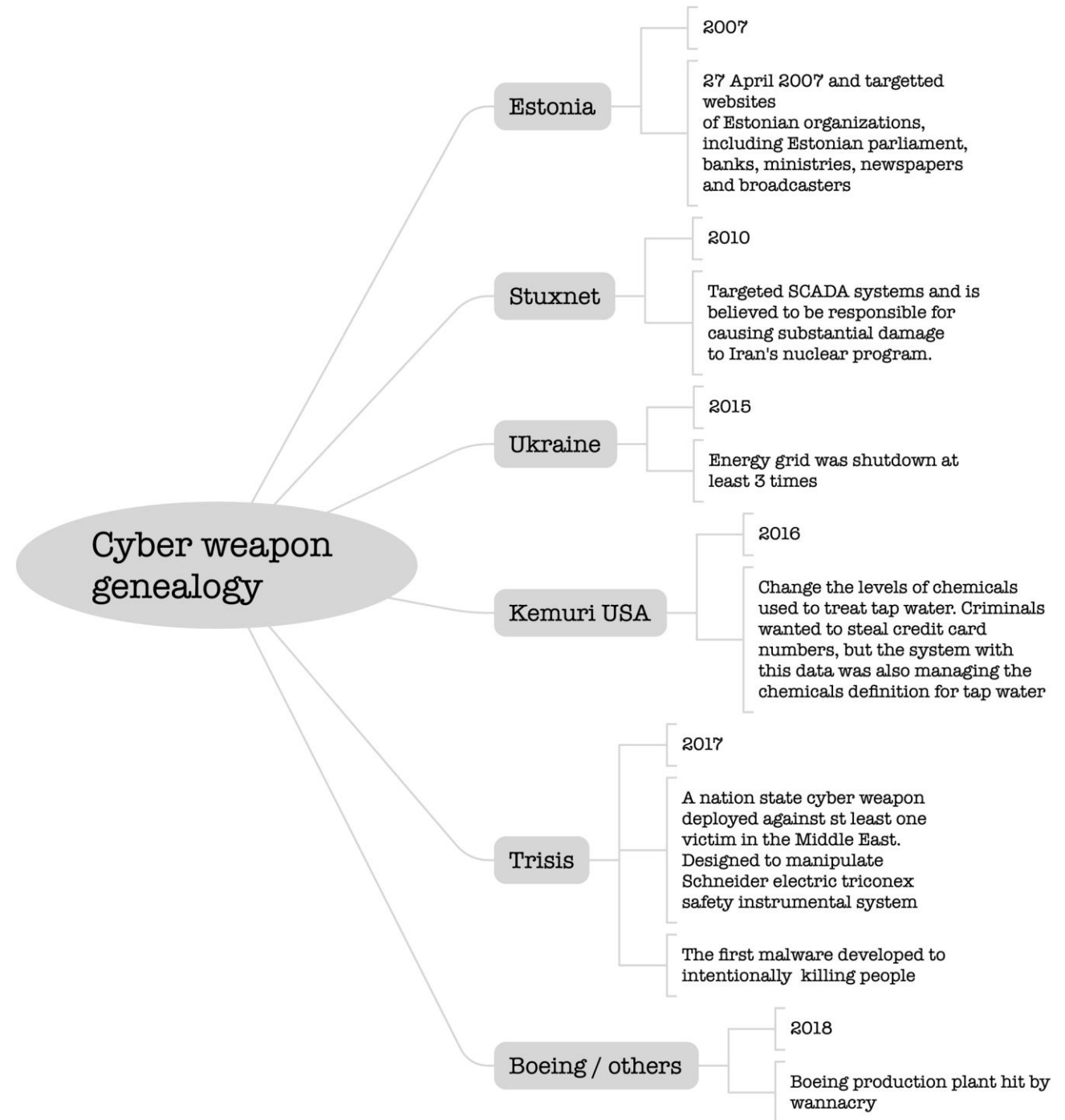
CHALLENGES/II



CHALLENGES/III: CYBER WEAPON

A cyber weapon:

- Is sponsored or employed by a state or non-state actor
- Meets an objective which would otherwise require espionage or the use of force
- Is employed against specific targets
- Its effects vary greatly with usage and time
- Unlike for instance CBR agents, cyber 'weapons' are neither banned nor controlled internationally.



SIX AI APPLICATION AREAS



Neural nets

- intrusion detection and intrusion prevention
- Used for DoS detection, malware detection/classification and in forensic investigations
- High speed, if implemented in hardware or used in graphic processors



Expert Systems

- knowledge base and inference engine
- Can be used used for decision support



Intelligent Agents

- Proactiveness and reactivity
- Imply cooperation between network operators (ISPs, etc)
- Could provide more accurate SA
- Automated or semi-automated response



Search

- Reduce a large number of options down to a manageable set
- Search on and- or trees, $\alpha\beta$ -search (“divide-and-conquer”), minimax search and stochastic search
- widely used in games software, highly useful in decision-making



Learning

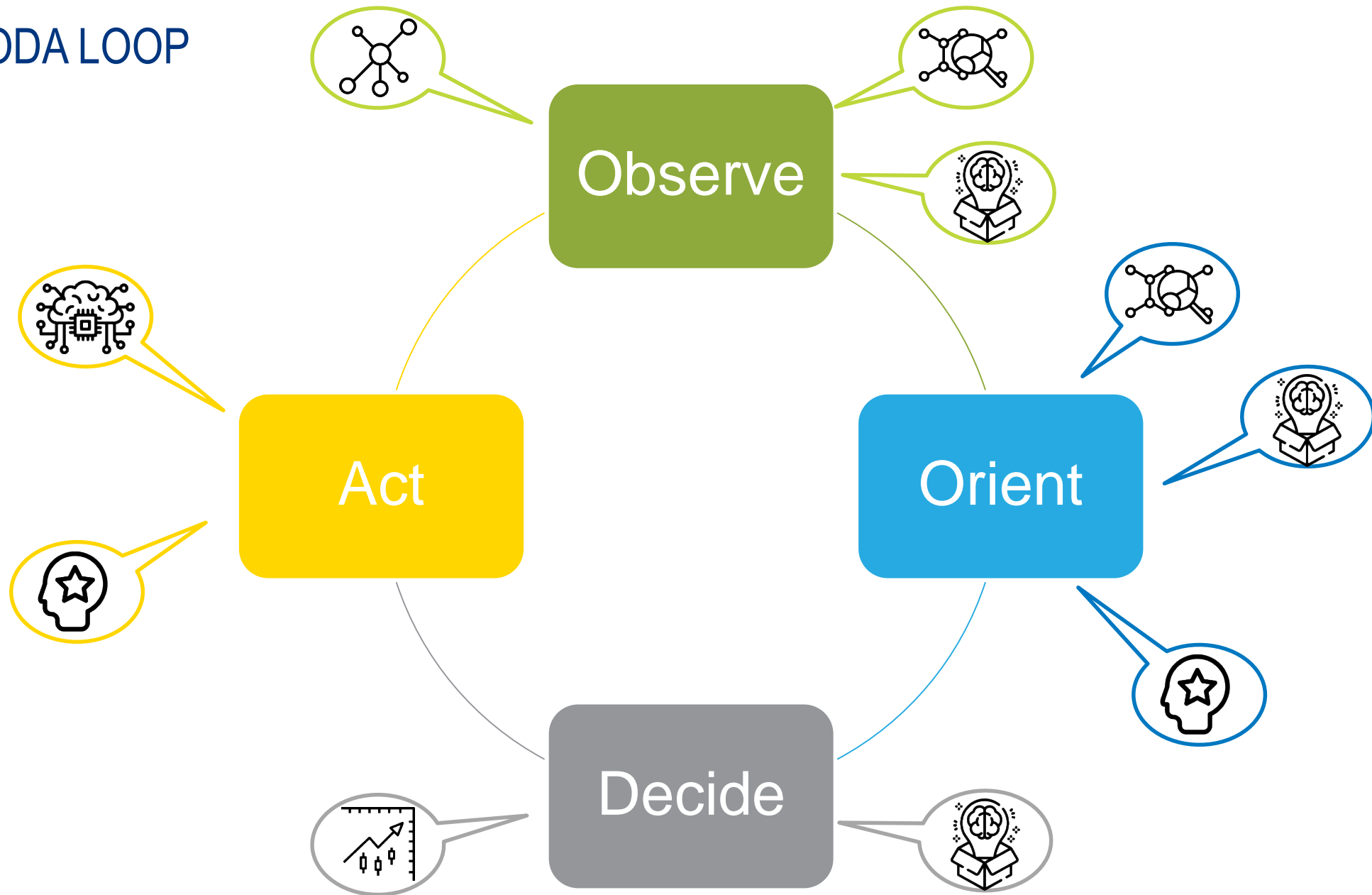
- improving a knowledge system by extending or rearranging its knowledge base or by improving the inference engine
- Supervised and unsupervised learning
- Useful to handle large amounts of data



Constraint Solving

- finding solutions for problems that are presented by giving a set of constraints on the solution
- Applicable to planning problems
- Can be used in situation analysis and decision support in combination with logic programming

THE OODA LOOP



CYBER DEFENCE TECHNOLOGY LANDSCAPING

Consortium ISDEFE, AIT, CEIS

Objective To identify technology challenges, enabling technologies, threats and discover gaps from Key Cyber Defence references.

To elaborate white papers, special reports, etc. with the research's results.

To propose possible Project Clusters of Cyber SRA elements.

To establish a framework to support EDA's Cyber R&T foresight activities

The output Will be used for the specification of new project activities

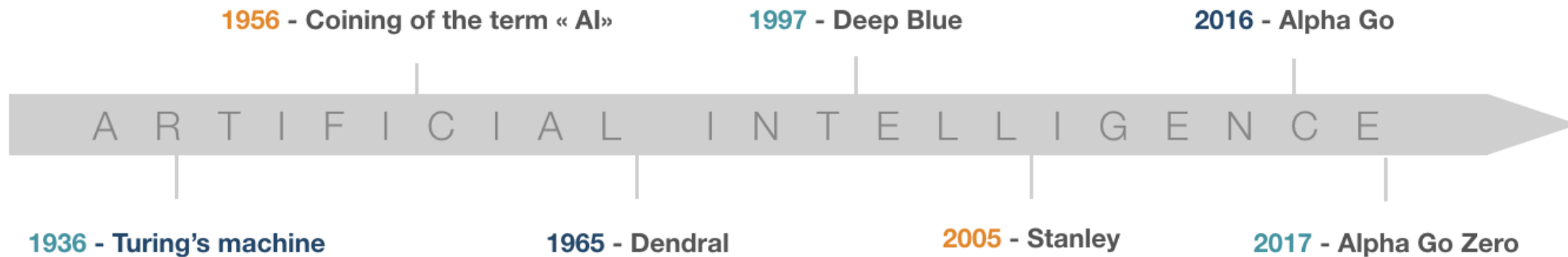


AI DEFINITION & CHARACTERISTICS

A.I.

A machine's ability to replicate functions generally attributed to humans, e.g. recognizing images or sounds**

Short story of AI



Speed / automation / real-time adjustment / large data set management

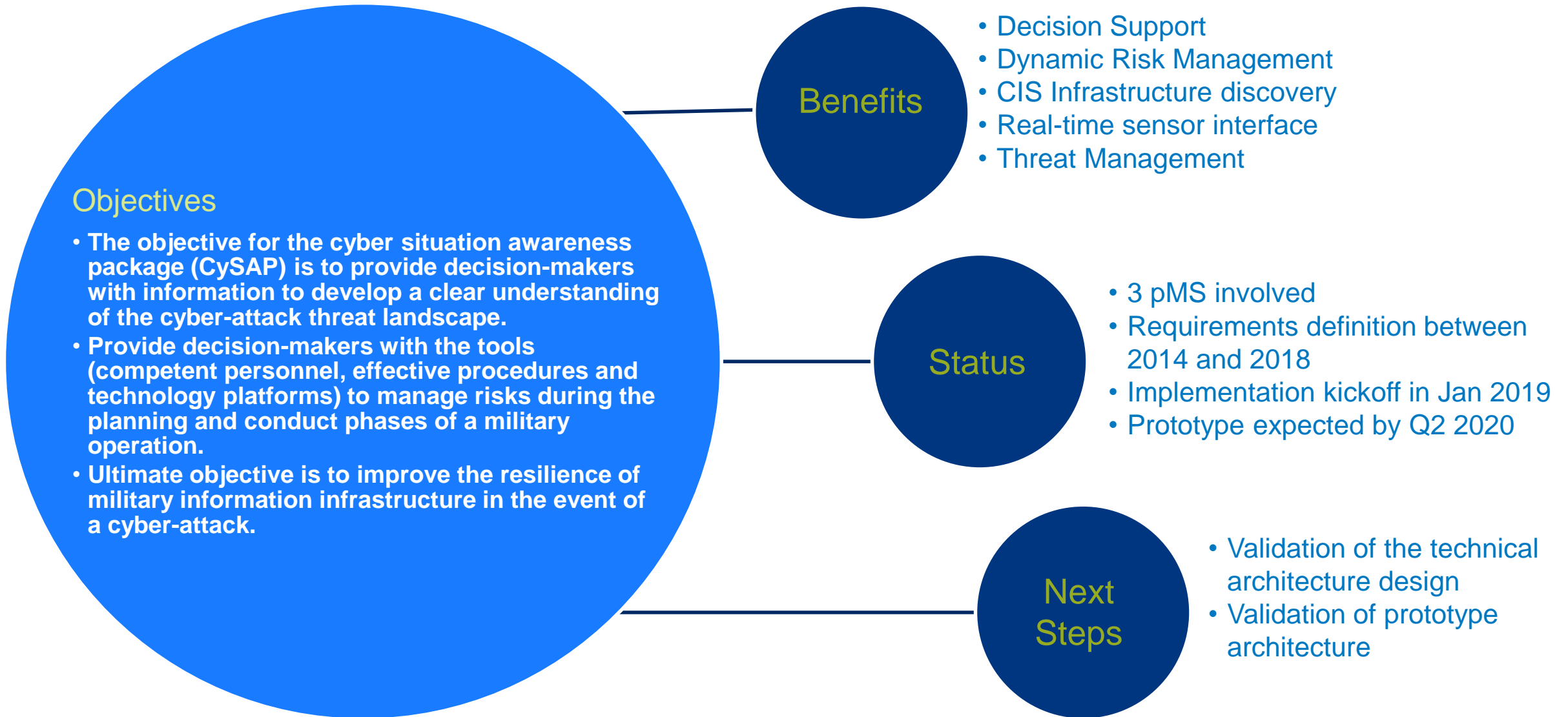
POTENTIAL APPLICATIONS

- Improving **resilience** – CHESS / combining human & machine strengths
- Early **detection** – GARD
- **Automation** of networks' management
- **Monitoring** of Internet Battle of Things devices



Food for thought

PROJECTS: CYSAP



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

THE POWER OF COORDINATION...



FOR MORE INFORMATION
WWW.EDA.EUROPA.EU

FOLLOW US ON TWITTER
[@EUDEFENCEAGENCY](https://twitter.com/EUDEFENCEAGENCY)

Thank you!