



Artificial Intelligence for Defence

F. Berizzi, Project Officer OPTRONICS technologies, EDA, Bruxelles

Colloquium on Artificial Intelligence and Big Data,
19 Mar 2019, Royal Higher Institute for Defence (RHID), Bruxelles, (BE)

OUTLINE

1. Defence research landscape

2. AI research issues

3. AI for Defence

4. AI in EDA

5. Conclusions

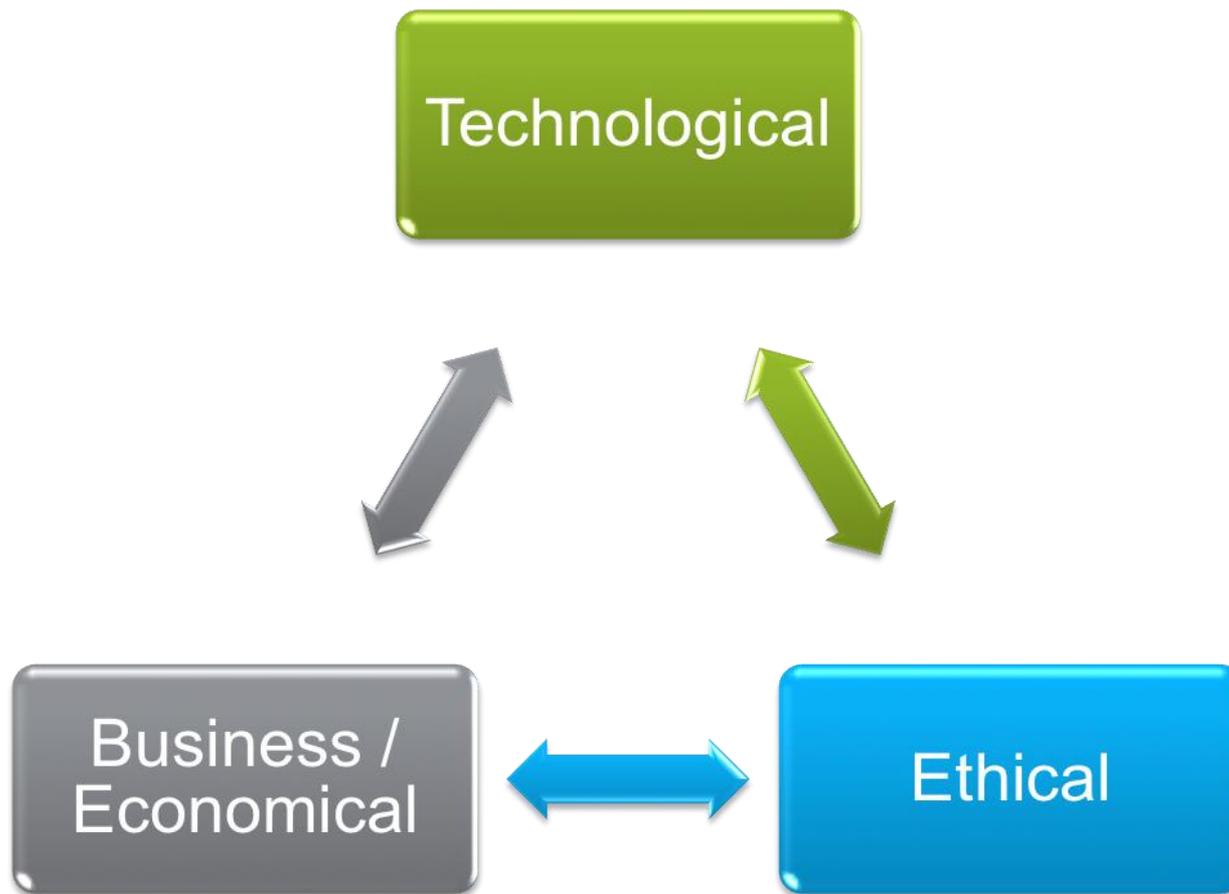


DEFENCE RESEARCH LANDSCAPE

Defence Research framework: Constant Changes



R&D in Defence Challenges



Evolving Threats: From Conventional to Asymmetric and Hybrid Threats

- Defence products need to be able to comply with a **diverse challenges coming from different operational scenarios**



Conventional



Asymmetric



Hybrid

Defence Business Market Structure

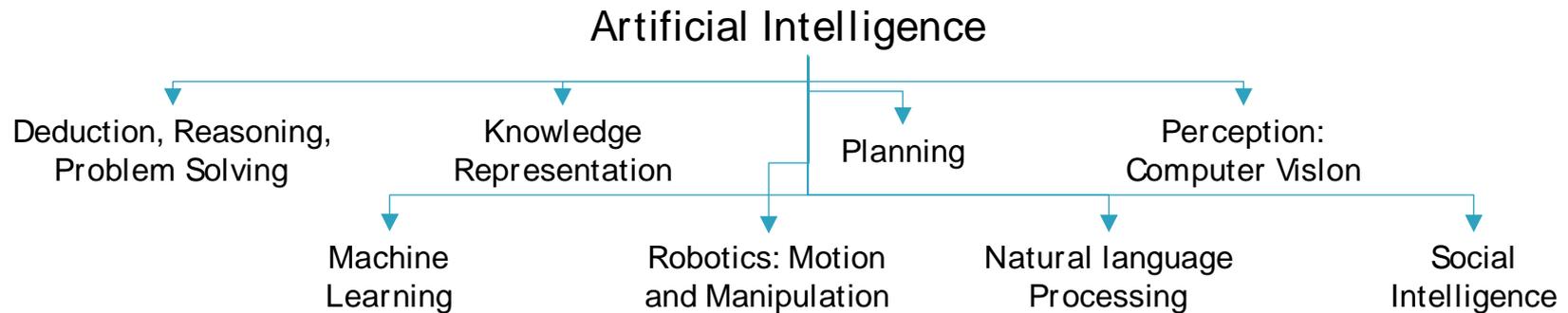
- Defence market is a **monopsony** market
- A market described as monopsony when **only one buyer interacts with many would-be sellers** of a particular product.
- In microeconomic theory of monopsony, **a single entity is assumed to have market power over terms of offer to its sellers**, as the **only purchaser** of a good or service, much in the same manner that a monopolist **can influence the price for its buyers** in a monopoly, in which only one seller faces many buyers.
- The **impact of this market structure** to R&D is manifold
 - **Barriers or high cost to entry**
 - **Regional focus**
 - **Lack of information**
 - **Inhibited Innovation**





AI RESEARCH ISSUES

AI R&D areas

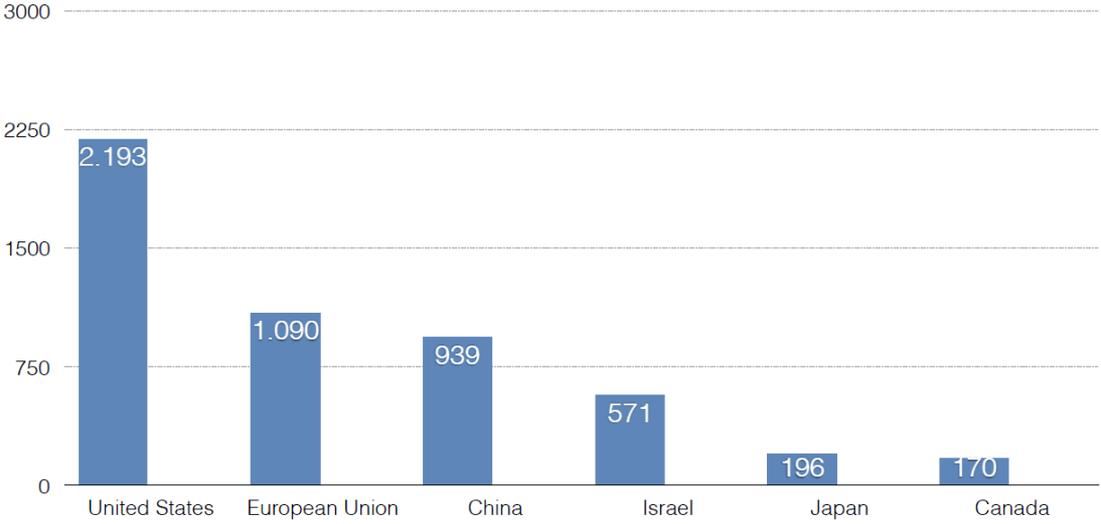


Based on Nazre and Garg, "A Deep Dive in the Venture Landscape of Artificial Intelligence and Machine Learning"

AI wide scope definition: "the study of the computations that make it possible to perceive, reason, and act"
(Patrick Henry Winston, *Artificial Intelligence*, 3rd ed., 1992.)

Business: Market Leaders

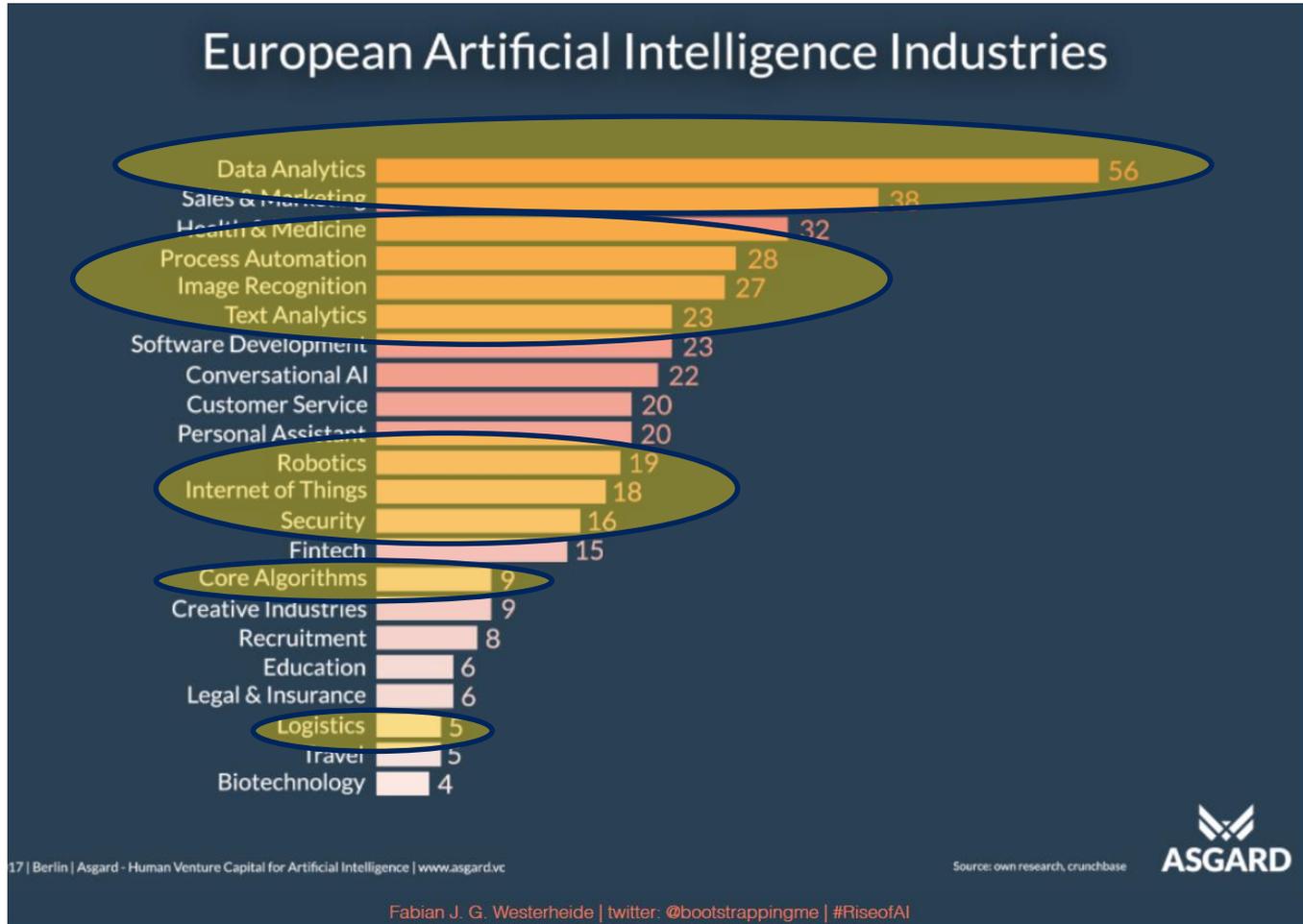
The USA is leading the AI market, followed by the EU



Source:Westerheide, Fabian J. G.: The European AI Landscape. Presentation at the European Commission AI Workshop, January 2018

Structure of AI ecosystem in EU

Defence Sector not represented



Compliance to Regulations /Standards



Ethical aspects for AI in Defence not yet formal

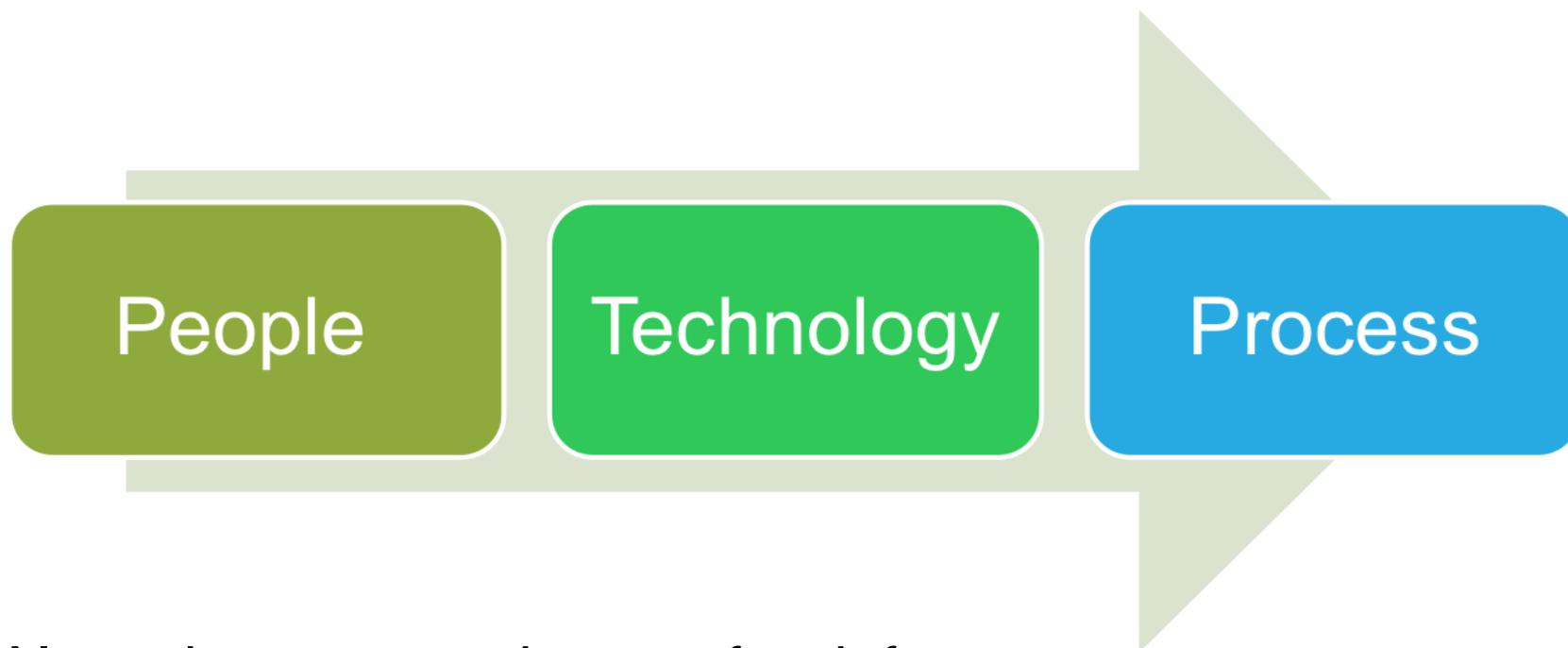


- An environment under development:
 - **Use AI enabled systems for support and managerial roles instead of combatant** role due to inability to:
 - discern between friend and foe
 - decide about the amount of force considered reasonable in a given situation.
- **Fears of a global AI arms race** that can lead to:
 - the emergence “on the black market of mass quantities of low-cost, antipersonnel microrobots that can be deployed by one person to anonymously kill thousands or millions of people who meet the user’s targeting criteria.” [article on/IEEE Spectrum](#)
- Key Questions to be answered:
 - Could autonomous armed robots perform more ethically than armed humans in combat?
 - Should we have a “kill” switch to every autonomous robot? (MEPs vote on robots legal status-Jan 2017)



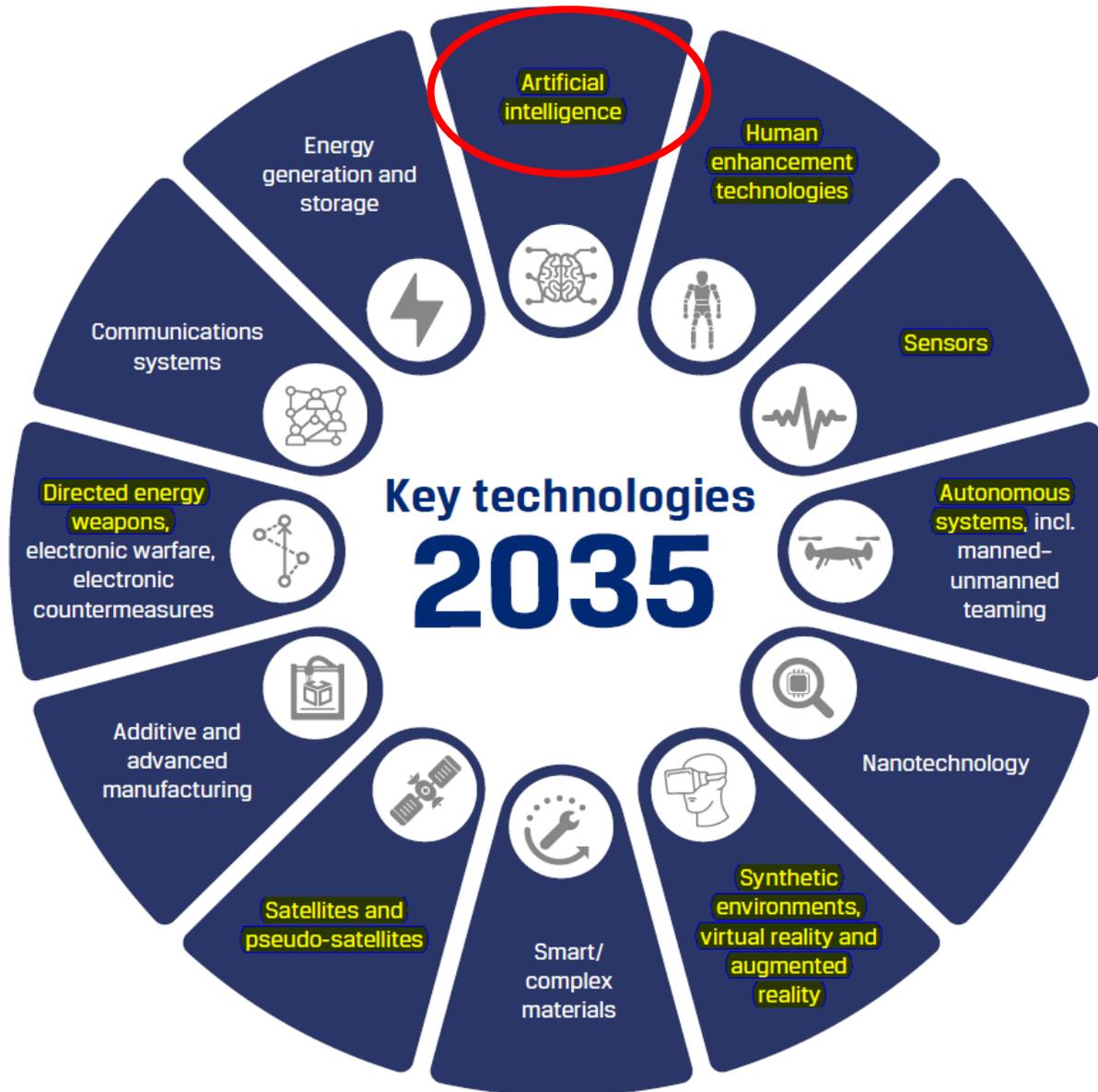
AI for DEFENCE

What AI is about for Defence?



- AI can be a game changer for defence:
 - **Reduces risk of life loss** in wars.
 - Can be **more efficient than regular soldiers**.
 - Are **less in cost about ten times** than the cost of human soldiers

KEY TECHNOLOGY 2035 + STRAND B



LONG TERM IMPACT ON MILITARY CAPABILITY 2035+ STRAND B



Information sharing
Efficient information sharing with joint multinational forces and with other military and civilian actors on the ground is an underlying requirement across all GMTLs



Decision-making
There is a need to ensure effective and rapid decision making at all levels, supported by enhanced situational awareness



Civil-military cooperation
Civil-military cooperation is necessary to ensure the fulfilment of the mission mandate in a complex environment



Mobility
Mobility is key to allow European forces to engage in more flexible and smaller deployments and operate in complex, contested and hazardous environments



Cyberspace
Cyberspace will become an ever-more integrated part of the physical battlefield



Non-lethal capabilities
Non-lethal weapons and systems development will allow for minimising collateral damage while disrupting the adversary's capabilities



Enhanced soldier
Enhancing individual soldier abilities is key for information gathering, mobility and resilience

AI Defence Research Domains



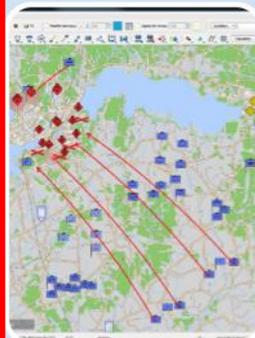
Cyber
Defence



Information
Management
and decision
making



Advanced
Analytics
-Deep
learning
-Machine
Learning



Modelling
Simulation
and Training

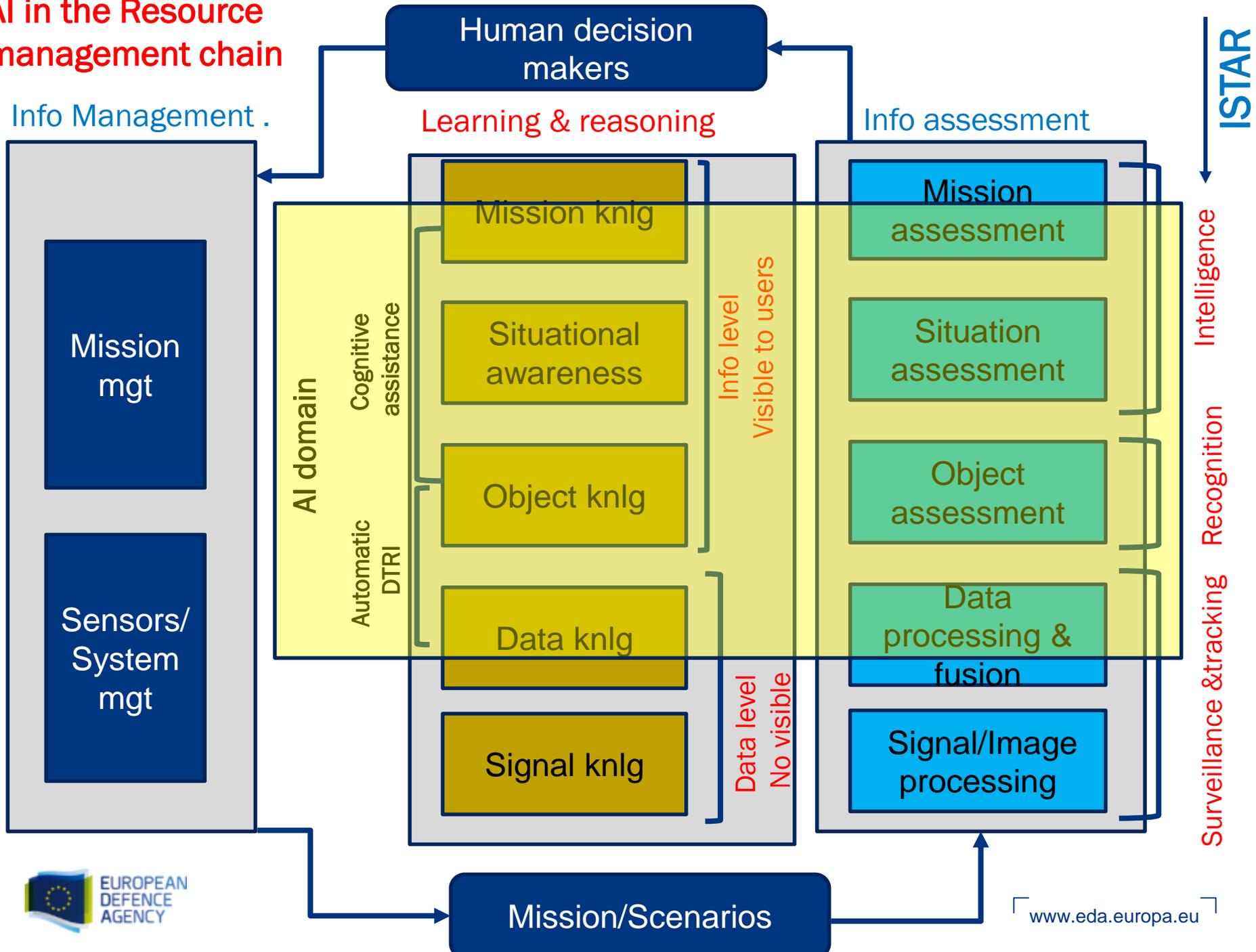


Autonomy
-Vehicles
(air,sea,land)
-Ammunition



Robotics
Support
(search and
rescue)
Logistic
Support
(carry
equipment)
Operate
(patrol,
destroy)

AI in the Resource management chain



AI generic technologies for Defence

1. Machine learning (ML) with/without human in the loop
2. Deep learning (DL)
3. Convolutional, Deep, Deep Convolutional, Recurrent NN (CNN, DNN, DCN, RNN)
4. Explainable AI (AI whose actions are easily understood by humans)
5. “Hard” data (multiple signals/images) fusion
6. “Soft” data (Observers, context, semantic, linguistic, taxonomy, ontology) fusion
7. Cognitive sensors
8. Integrated hardware accelerators

AUTOMATIC DTRI

- Background/clutter cancellation
- Object classification and recognition
- Super-resolution
- Change or anomaly detection
- Multisensor signal/image (“hard” data) fusion
- Counter IED

Cognitive assistance (Aid decision making)

- Knowledge based assistance
- Cognitive modelling for adaptive training
- Observers, context, semantic, linguistic, taxonomy, ontology (“soft” data) fusion
- Internet of Battlefield Things—IoBT (Future battlefields to contain millions of networked devices)

AI potential gaps

1. AI&ML/DL robustness and efficiency with small samples, dirty data, high clutter
2. ML and/or DL that is Robust and Resistant to Deceptive and Conflicting Inputs (adversarial)
3. Reasoning about enemy that incorporates distributed learning
4. Adaptive Real-time Learning with Constrained Resources
(limited comms, Resource-constrained adaptive computing)

Need of an AI Taxonomy to facilitate research in EU



Interoperability and Common Understanding

- The range of cooperation based on AI can be better understood based on a common AI Taxonomy and definitions

BENEFITS

- Establish a common understanding and facilitate discussions
- Have a solid basis to organize and coordinate future projects
- Improve communication between stakeholders



OUTCOME

- Taxonomy as a common European basis to start analysis of AI Defence needs
- Common mindset to discuss on potential projects based on a solid taxonomy with the understanding of the needs as key to success



AI in EDA

AI in EDA: highlights

48 related
OSRA
TBBs

1 related
CDP priority

1 technology
foresight
workshop

3 experts
Workshops

EDA
Innovation
Prize

AI in EDA: some details

Workshop on “Artificial Intelligence for OPTRONICS systems”
22.10.2018, EDA

Workshop on “ AI and Cognitive Technologies for Radar, Comms and EW, 3 and 4 December 2018, EDA premises, Brussels

Technological foresight WS on artificial intelligence, 13-14 Dec 2018, EDA, Bruxelles

14 OB studies launched or to be launched on AI related topics in 2014-2019

8 EDA Cat B & Cat A related projects

1 Workshop on AI taxonomy and high level applications for Defence (Q3 2019)

AI Foresight workshop results

Key Messages From AI (1/3)

- AI is a **transformative technology** which will impact many of the future systems and **military applications**.
- Although clear applications in systems as the FCAS (Future Combat Air Systems) can be identified in the long run, the **key applications identified** as the earliest and with most likelihood and impact in the short run. They are
 - **Decision making in C2,**
 - **Intelligence gathering**
 - **Autonomy**

Some examples are :

- Reasoning plus contextual understanding techniques to enhance the “common sense” in the current AI developments
- AI driven **smart** cognitive sensor **network** combined with Smart **and secure** communications and channel management. Active learning in real time.
- Machine learning in engagement

Key Messages From AI (2/3)

- These applications need of three fundamental challenges:
 1. The **establishment / development of technological and organizational capabilities** in the:
 - i. Verification, Validation, Certification and Trust & Confidence building of AI systems, also including the identification and assessment of the vulnerabilities derived of the organizational implications of AI.
 2. **The collection of data to support the (constant) training of the machines.** This collection has several aspects of consideration:
 - i. Procedural aspects in the collection among different European countries. Difficulty in a European level Database.
 - ii. Data sovereignty (country data parcellation, confidence level parcellation, data integration,...)
 - iii. Access to very specific data (because of the sensitive application/source, or because of lack of data).
 - iv. Data lifecycle and database management in the defence context
 - v. The significant effort needed to train and label data.

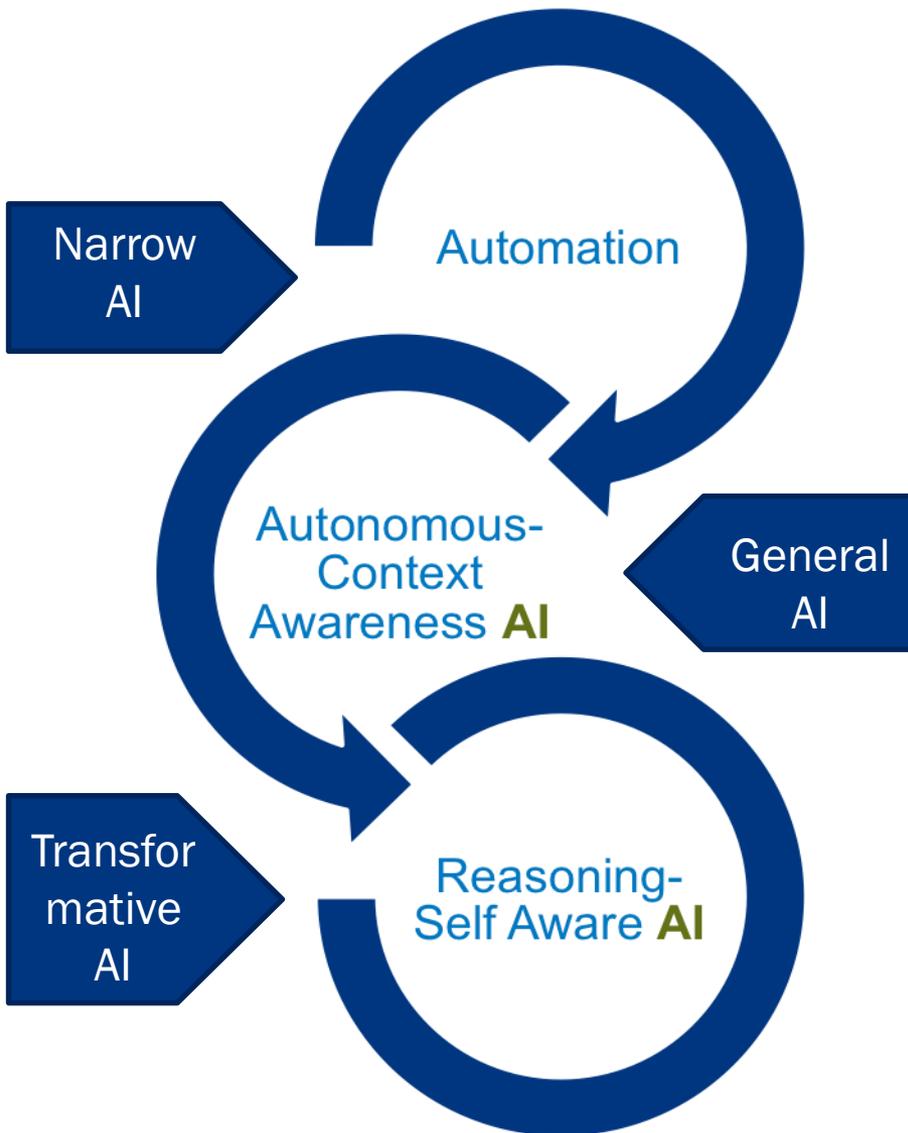
Key Messages From AI (3/3)

- These applications need of three fundamental challenges:

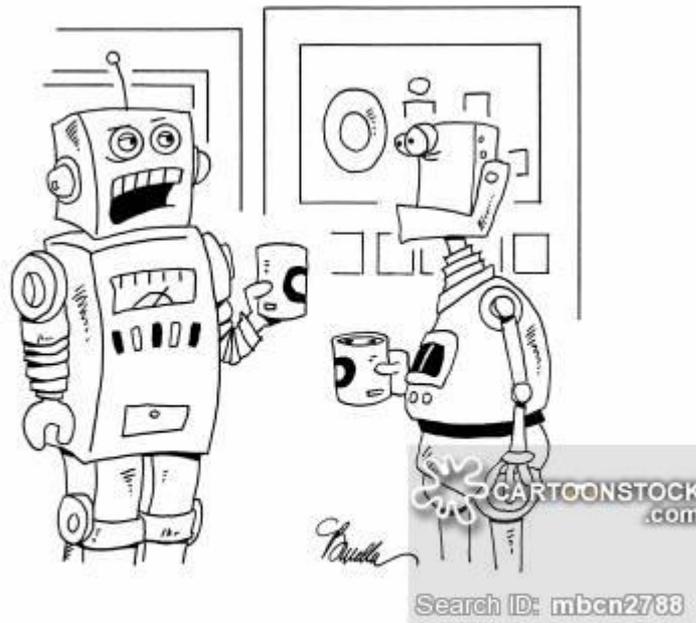
3. The maturation of the following technological aspects:

- Robust and distributed Machine learning
- Knowledge representation (build shared ontology, lifecycle of knowledge representation,) and understanding of cognitive states and its impact on human machine interfaces.
- High performance edge computing
- The specialization in AI of existing/new methods and tools to model, design & simulate new developments in AI.

Looking to the future



- As the AI research evolves, so do AI applications in the military, e.g. RPAS → Autonomous UAV → Self-Aware Drones → Drone Swarms (e.g. Perdix)
- AI is an enabler; but it will also disrupt the current military structures → the disruption will be horizontal and vertical → flexibility and adaptation needed
- Impact in balance of power vis-à-vis military operations (first user advantage, adoption capacity theory)
- Disruption in military organisational and cultural infrastructures (both in war and peace times)
- Balance of innovation and application between civil-military → impact on interoperability



"Sure, it seems harmless, but you hire one human and the next thing you know, they're taking your job."

Questions?