R1.2 ANNEX 2 - Brainstorming sessions with industrial experts for the Defence Technology Roadmap

Dissemination level: PU (public)

Co-funded by the Erasmus+ Programme of the European Union

Index

Figure index

Table index

The **Technologies Roadmap** (R1.2) is a **twin document** with the **Skills Blueprint** (R1.3).

Those documents describe the **current landscape** and the **future trends** within the technological domain of Robotics, Autonomous Systems, AI, Cybersecurity, and C4ISTAR in the Defence sector.

In particular, the **technologies** and their defence-related **applications** are analysed, then the impacts on **skills** and **job profiles** are discussed.

As twin documents, they **share** some contents:

This is a **joint annex**.

With the support of the
Erasmus+ Programme
of the European Union

1. Introduction

The ASSETS+ project is aims at creating a strategy to up-skill defence students and professionals, including the identification and standardization of job profiles related to the technologies identified in this project. This document belongs to the WP1 of the project and is part of a broader effort to analyse technology and skills focused on the context of defence.

The work is divided in three macro technological areas, each one analysed by a part of the WP1 team:

- **Robotics, artificial intelligence (AI) and autonomous-systems**: addressed by *Aalborg University* and *Rzeszów University of Technology*;
- **C4ISTAR**: addressed by *Bordeaux University* and *Pisa University*;
- **Cybersecurity**: addressed by *Carlos III University* and *Seville University*.

This document contains: a description of the industrial needs within the defence sector, an overview of the current state of the educational programmes related to defence, the roadmaps that describe the expected evolution of the technological domain within the defence sector.

The roadmaps derive from blending big data, collected and analysed with automatic data-driven analysis, and experts' knowledge, gathered during brainstorming sessions with industrial experts.

This document presents the results of the brainstorming sessions executed with technical experts from defence industry.

The brainstorming sessions results consists of identifying and classifying the ideas developed by the technical experts during structured brainstorming sessions dedicated to foreseeing the future oriented time-framed relations of technologies, applications, job activities and education and training activities.

2. Results from brainstorming sessions

This paragraph presents the results of the three brainstorming sessions executed with the technical experts from the ASSETs+ Consortium.

The domains within the scope of ASSETs+ are C4ISTAR, Cybersecurity, Robotics, Artificial Intelligence and Autonomous Systems. The analysis of these domains is complex, given that these are strongly entangled. To overcome this entanglement, and to have a theoretical sounding but also actionable framework, we propose an updated version of C4ISTAR, a so-called 4.0 version: C4AID. This is an acronym that stands for "Command, Control, Communication, Cybersecurity, Artificial Intelligence, in Defence". This framework is for us the natural evolution of C4ISTAR, given that it contains all of the elements that the previous framework was containing. This novel framework will be used to look at the ASSETs+ technologies and applications a holistic and future-oriented way. It has the form of a matrix containing the relevant technologies for ASSETs+ project, and the relevant defence areas. The framework is reported in the Figure 1.

C4AID: Command, Control, Communication, Cybersecurity, Artificial Intelligence, Defence (Intelligence, Surveillance, Target Acquisition, Reconnaissance)		Defence Areas					
		Factory	Land	Sea	Air	Space	Cyberspace
Technologies	Artificial Intelligence						
	Cybersecurity						
	Robot						
	Autonomous Systems						

Figure 1 - Framework C4AID (Command, Control, Communication, Cybersecurity, Artificial Intelligence, Defence: Intelligence, Surveillance, Target Acquisition, Reconnaissance).

The C4AID framework presents:

- on the rows, the technological fields under analysis in ASSETs+: Robotics, Artificial Intelligence, Autonomous Systems, and Cybersecurity.
- on the columns, the main areas of the Defence sector: factory, land, air, sea, space, and the cyber-space.
- on the intersections, the applications of a technology related to a given domain a specific Defence sector.

The C4AID framework allows to take into consideration both the interrelation between the technological fields (i.e., rows) and their connections to the Defence sector (i.e., columns). This will help in harmonizing the WP1 outputs to the specific needs of the sector.

The organization of the brainstorming sessions is based on the framework C4AID, in particular we grouped the experts based on the intersections[1]. The executed sessions are the following:

1. **The impact of the technologies of the domains Artificial Intelligence, Robotics and Autonomous systems in the Sea Defence Area**
2. **The impact of Cybersecurity in Defence areas (Air, Naval, Space, Sea, Cyberspace and Factory)**
3. **The impact of Artificial Intelligence in Defence areas (Air, Naval, Space, Sea, Cyberspace and Factory)**

Each of the following sections describes the outcomes within a specific session.

[1] The brainstorming sessions do not address all the intersections of the framework C4AID. This might imply that the full spectrum has not been properly covered. However, during the execution brainstorming sessions, some overlaps emerged in the comments of the experts collected. In addition, some of the technical experts indicated by the companies were involved twice in the sessions, so the collected ideas couldn't be so different. Therefore, these overlaps indicate that collected information might refers to more than one intersection, allow us to cover the full perspective.

2.1 The impact of the technologies of the domains Artificial Intelligence, Robotics and Autonomous systems in the Sea Defence Area

This brainstorming session involved 6 technical experts from 5 different companies of the ASSETs+ Consortium.

They generated 48 different ideas in the 3 parts within the brainstorming session. The parts were dedicated to technologies and applications, job activities, education and training. The virtual boards of each part are reported in the Figures 2, 3 and 4.

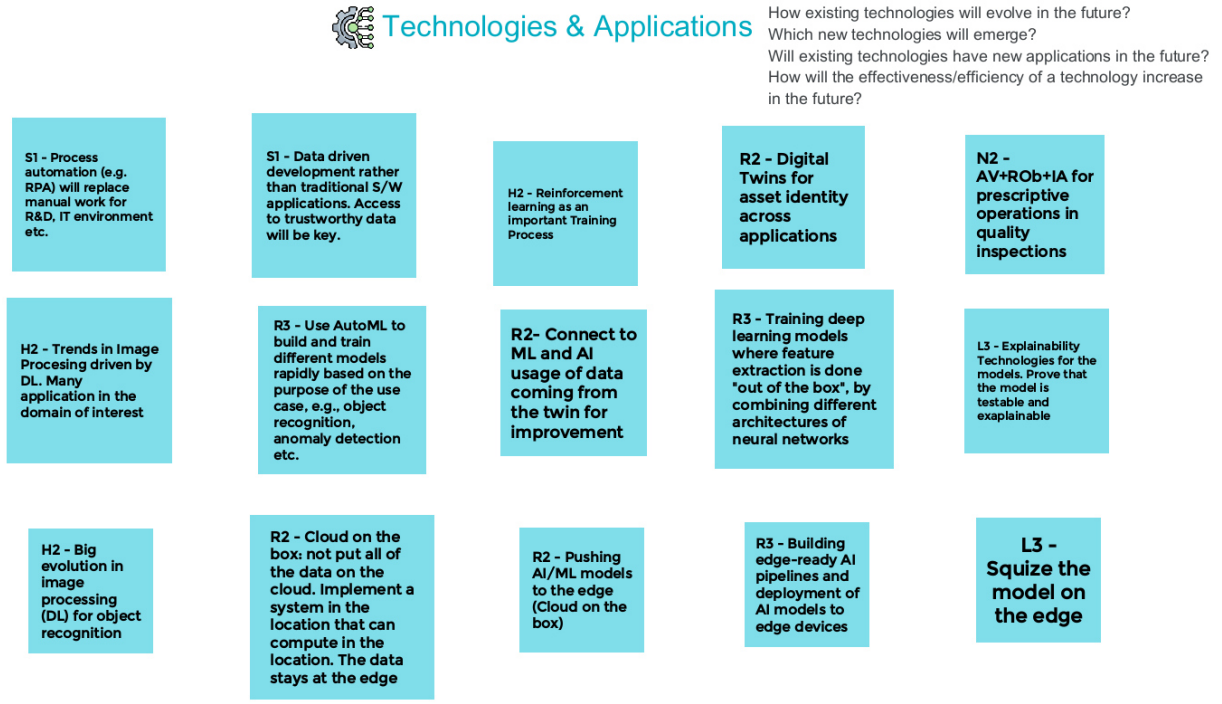

Figure 2 - Board for the technologies and application part in the brainstorming session on "The impact of the technologies of the domains Artificial Intelligence, Robotics and Autonomous systems in the Sea Defence Area".

Figure 3 - Board for the job activities part in the brainstorming session on "The impact of the technologies of the domains Artificial Intelligence, Robotics and Autonomous systems in the Sea Defence Area".

Figure 4 - Board for the education and training part in the brainstorming session on "The impact of the technologies of the domains Artificial Intelligence, Robotics and Autonomous systems in the Sea Defence Area".

The experts' ideas are compared with the technologies and applications identified in the data-driven analysis with the purpose to detect the missing elements.

The Table 1 summarises the list of identified technology, related technologies from the technology roadmap, and explanations/comments. Note that the colours refer to the following:

- **Red:** technology not included in the latest version of the technology roadmap report.
- **Orange:** relevant technology, but already exists as a combination of technologies or in a more generic terminology.
- **Green:** technology already included in the technology roadmap report.

Table 1 – Table of technologies observations derived from the brainstorming session on "The impact of the technologies of the domains Artificial Intelligence, Robotics and Autonomous systems in the Sea Defence Area".

Technology	Corresponding technology current roadmap (if any)	Comment/Specific application
Process automation	Automation	• Automation of monitoring of infrastructure and cyber-security activities. • Access rules for accessing application/digital services
Image processing	Related technologies: • Image Semantic Segmentation • Computer vision • Machine learning • Deep learning	Application of ML and DL for image processing tasks: • 3D image processing • Object recognition and classification • High perceptual representation of a scenario • spectrometer (IR images)
Digital twin	Loosely related to: • Simulation • Optimisation	Designing a digital clone of physical assets: • Two-direction information flow • Use data obtained from the digital twin as input for AI algorithms to analyse physical assets • Cross-application asset identity
AI-based/Data-driven software development	• Artificial intelligence • Machine learning • Deep learning • Reinforcement learning • etc.	Use data for software development (SD) processes: • Data access • Ensure data quality • Monitor the training data • Implement features driven by data /!\ This is not a technology as it looks more like a skills/job function. However, this task can be achieved using a mix of the technologies shown in column 2 (from the technology roadmap)
AutoML	• Artificial intelligence	Automate the training process for ML algorithms: • Parameter tuning • Automated model generation

Technology	Corresponding technology current roadmap (if any)	Comment/Specific application
	• Machine learning • Deep learning • Reinforcement learning • etc.	• Model optimisation
Building edge-ready AI algorithms and deployment of AI models to edge devices	• Edge computing • Artificial intelligence • Machine learning • Deep learning • Reinforcement learning • etc.	"Edge computing meets AI" • Building AI algorithm on edge infrastructures which is independent from external information sources and computing resources
AV+ROb+AI for prescriptive operations in quality inspections	• Artificial Intelligence • Autonomous-system • Robotics	• carry out the inspections in the production process, both for the systems and the product • Substitute the manual operations with robots • Develop AI algorithm to teach the robots how to operate and to control the robots as well
Training deep learning models where feature extraction is done "out of the box", by combining different architectures of neural networks	• Artificial intelligence • Machine learning • Deep learning • Reinforcement learning • etc.	Combining multiple DL algorithms to solve complex problems
Cloud on the box	• Edge computing • Artificial intelligence • Machine learning • Deep learning • Reinforcement learning • etc.	Localise the deployment of ML/AI algorithms (ease of data processing, avoid cybersecurity issues, easy to transport the models, etc.)

Technology	Corresponding technology current roadmap (if any)	Comment/Specific application
Explainability Technologies for the models	• Exokainable Artificial Intelligence (XAI)	Ensure that the AI algorithms are explainable and testable: • For certification of the product • For ensuring testability
Squeeze the model on the edge	• Edge computing • Artificial intelligence • Machine learning • Deep learning • Reinforcement learning • etc.	Embed AI on edge devices to elaborate directly the data (that are on the edge).
Big evolution in image processing (DL) for object recognition	• Deep learning • Machine learning • Computer vision	Similar to “Image processing”

Based on the analysis of the abovementioned technologies, two technologies were identified:

- **Digital twin:** this is loosely related to simulation (as it is about creating/simulating a clone of a physical system), and to optimisation (optimisation of parameters of a process realised on an asset).
- **Image processing:** this is related to technologies that are existing in the latest version of the technology roadmap, namely, computer vision and image semantic segmentation. However, the existing technologies might not cover specific image-related applications such as IR image processing, 3D images, etc.

In addition, other technologies that are relevant were mentioned, these technologies are special cases or a combination of technologies existing in the latest version of the technology roadmap. We cite among others:

- AI on edge devices
- Process automation
- Auto Machine Learning (AutoML)

The first technology is particularly important and relevant to the particularity of the defence sector. Advantages of bringing AI to edge devices include: low energy consumption, localised data processing, low cost, low latency and data safety and security. We identify the following related and more specific technologies:

- Federated learning: implementation of AI algorithms on decentralised edge devices
- Frugal AI: AI under scarce computing resources and potentially limited data.

Finally, it is reminded that Machine Learning should therefore be identified as a technology for the topic of Artificial Intelligence, also for Big Data.

Some additional elements:

- Advanced Optimisation and Anomaly Detection/ Time Series are missing. Those are specific AI methods and approaches that are quite relevant
- Mentioned and needs particular attention: certifiable/ trustworthy AI
- Cloud is mentioned, however only in the perspective of major cloud providers. A trend (GAIA-X) is that Europe is more and more striving for more sovereignty and a multi-cloud approach. So this is a skill need that is not reflected. A strong cloud capability is a key pre-requisite for the industrialisation of AI and automation solutions.
- Another key enabler for the industrialisation of AI solutions is a strong data ontology (semantic representation of data) and data architecture/modelling capability.
- The brainstorming paper is looking at the technical skillsets needed for the AI professionals. Nevertheless, it is worth including the aspect of User-Experience and HMI. Whenever we talk about automation, or a model prescribing a solution/action to the end-user, it is key that it remains intuitive and easy to understand for the ultimate end-user so that even in stress situations, the end-user (e.g. pilot) can easily process information/ insights given.
- Image Processing could be extended to "Signal processing" (For analysis and processing radar, sonar,
  radio signals), for which Data fusion is also an important application

Job Activities Roadmap

Based on the outcome of the brainstorming activities, we distinguish the following job activities:

- Development of application-focused, data-driven tools and decision support systems; and create models ready for production.
- Study research papers to stay on track with emerging technologies and be able to transfer knowledge from the civil sectors to defence.
- Develop interdisciplinary skillset on DevOps, software engineering, AI and data science.
- Ethical supervision and evaluation of technologies.
- AI engineers should have close communications with the defence experts.

Education and Training Roadmap

The brainstorming resulted in the following recommendation from industry experts:

- Education for active engineers:
  - Upskilling and reskilling.
  - Enable peer-to-peer learning across industries.
  - Enrol in training programmes and certification by cloud providers such as AWS, Google Cloud, MS Azure, etc.
- Strong technical training:
  - Include more simulation methods and tools more in education to help young talents acquire the necessary knowledge to be able to support the digital transformation in industry (digital twins, complex simulation environments, etc.).
  - Include data science-focused programming languages such as R and Python, and toolboxes in training programmes.

- Technology stack education: data storage, message brokers, distributed processing, computing clusters, open-source solutions such as MLflow for model serving and registry, containerisation via Docker, etc.
- Strong mathematical foundations for data scientists, mainly in statistics and stochastic systems.
- Technical training for leaders: leaders should be informed on new technologies and trends in AI and machine learning.
- Include industrial applications and problems in education.
- Encourage multidisciplinary in defence education.

2.2 The impact of Cybersecurity in Defence areas (Air, Naval, Space, Sea, Cyberspace and Factory)

This brainstorming session involved 5 technical experts from 5 different companies of the ASSETs+ Consortium.

They generated 59 different ideas in the 3 parts within the brainstorming session. The parts were dedicated to technologies and applications, job activities, education and training. The virtual boards of each part are reported in the Figures 5, 6 and 7.

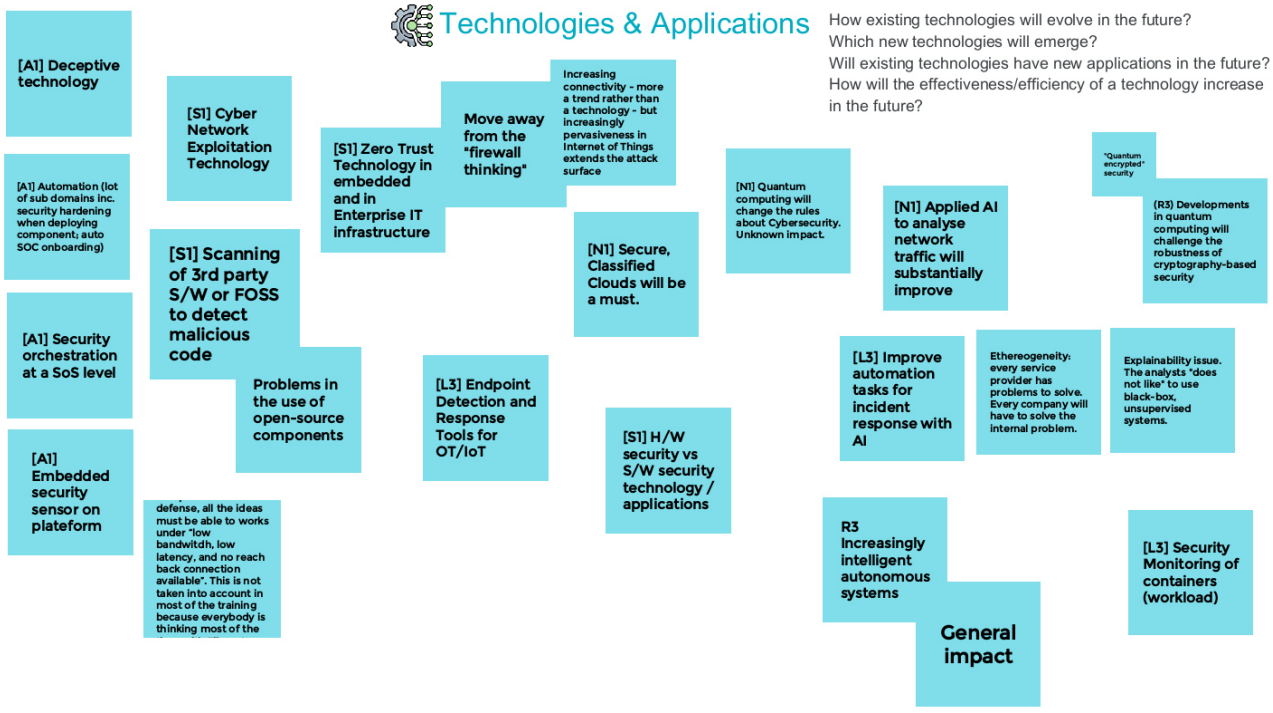

Figure 5 - Board for the technologies and application part in the brainstorming session on "The impact of Cybersecurity in Defence areas (Air, Naval, Space, Sea, Cyberspace and Factory)".

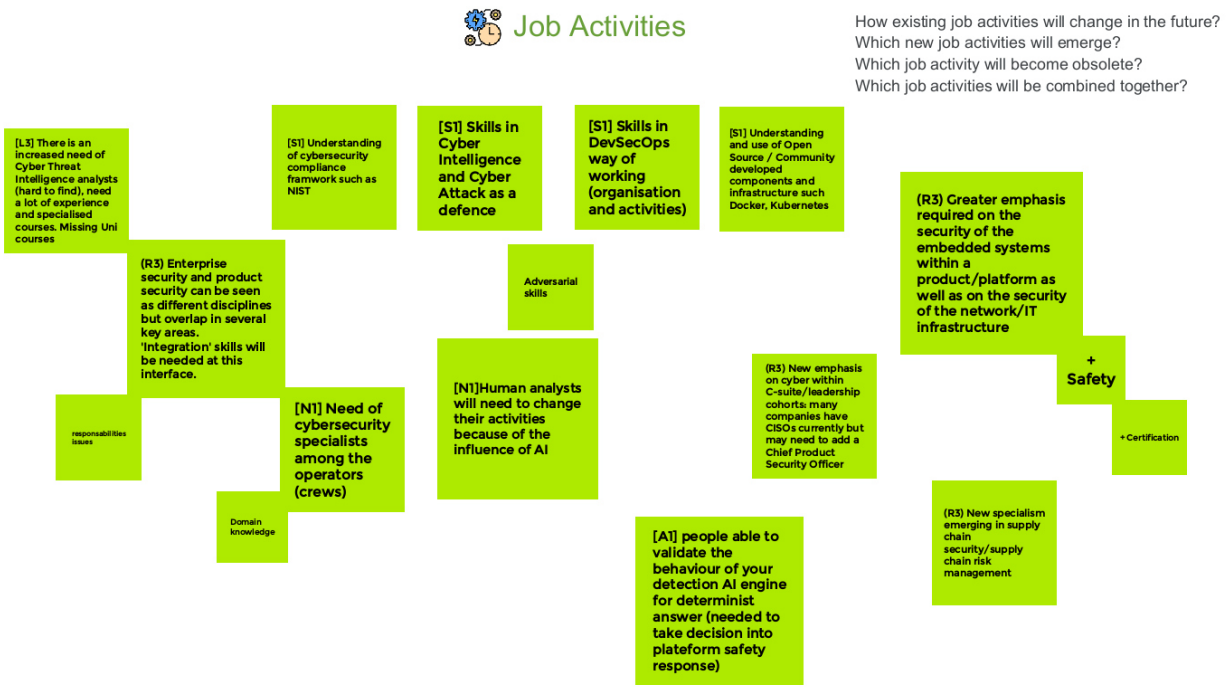

Figure 6 - Board for the job activities part in the brainstorming session on "The impact of Cybersecurity in Defence areas (Air, Naval, Space, Sea, Cyberspace and Factory)".

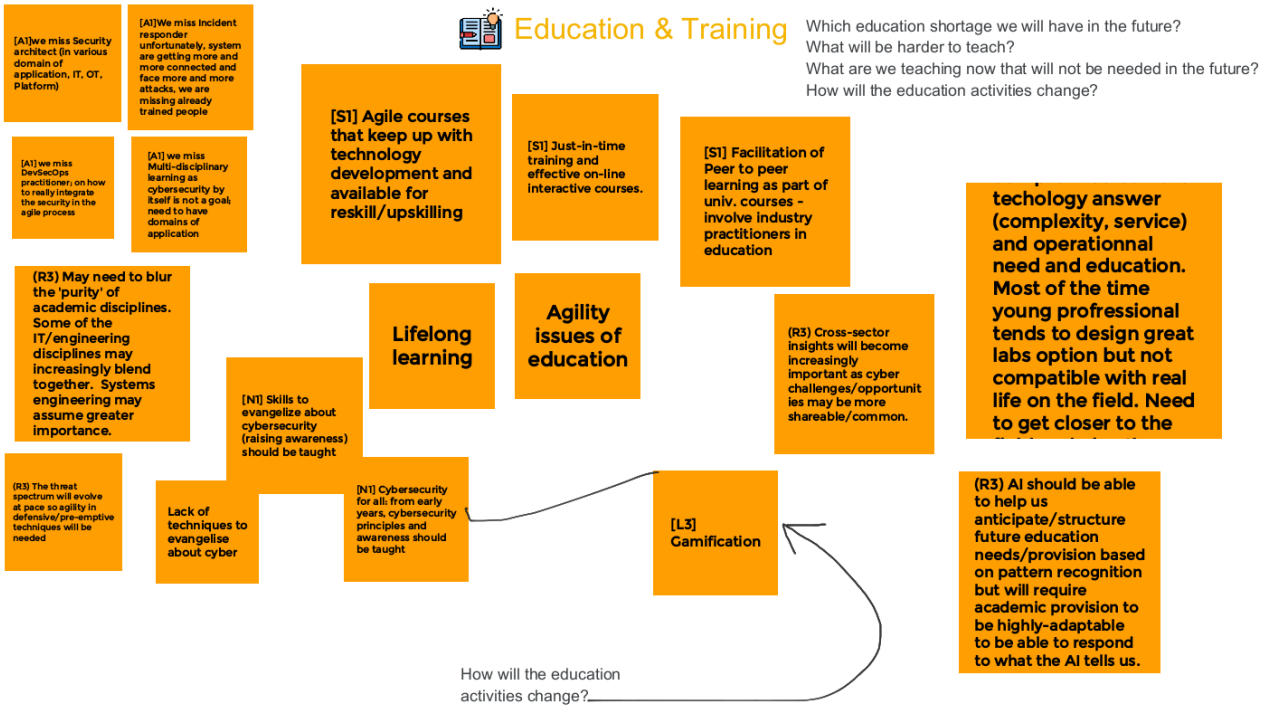

Figure 7 - Board for the education and training part in the brainstorming session on "The impact of Cybersecurity in Defence areas (Air, Naval, Space, Sea, Cyberspace and Factory)".

The experts' ideas are compared with the technologies and applications identified in the data-driven analysis with the purpose to detect the missing elements.

The Table 2 summarises the list of identified technology, related technologies from the technology roadmap, and explanations/comments. Note that the colours refer to the following:

- **Red:** technology not included in the latest version of the technology roadmap report.
- **Orange:** relevant technology, but already exists as a combination of technologies or in a more generic terminology.
- **Green:** technology already included in the technology roadmap report.

Table 2 - Table of technologies observations derived from the brainstorming session on " The impact of Cybersecurity in Defence areas (Air, Naval, Space, Sea, Cyberspace and Factory)".

Technology	Corresponding technology current roadmap (if any)	Comment/Specific application
Deceptive technology	Honeypots	• To be used in your network to take automatic decisions against attackers
Embedded security	Related technologies: • Mobile & IoT security • Hardware security	• Relevant within a network or product • Safety paramount • Certification is demanded
Zero Trust technology	Related technologies: • Firewalls • Honeypots • Identification & authentication • Authorization & access control	• Critical in embedded and enterprise IT infrastructure. • Move away from “firewall thinking.”
Endpoint detection	Endpoint security	
Secure cloud	Cloud and virtualization security	• Information classification should be protected
Quantum computing	Related technology: • Encryption	• The impact is unknown – likely high. It will be a game-changer in cybersecurity • Crypto mechanisms are a challenge
AI for cybersecurity	Related technologies: • Endpoint security • Malware analysis • Cyber threat intelligence • Firewalls	Applications of AI to: • Incident response management • Traffic analysis • Cybersecurity processes automation (smart decisions) In some cases, e.g., validation of detection engine, human knowledge/tasks are needed
Network exploitation	Related technology: • Penetration testing • OSINT/PRIVINT	
Cyber threat intelligence	Cyber threat intelligence	• It is crucial for defence • There is a need for this type of specialists – not coveredUniversity courses exist, just SANS

Technology	Corresponding technology current roadmap (if any)	Comment/Specific application
Secure software development	Secure software development	• Understanding and using open -source / community-developed components and infrastructure such as docker, Kubernetes • There are problems in the use of open source components, particularly to detect malicious code.
Supply chain security	Related technologies: • Mobile & IoT security • Certification • Risk assessment and management • Compliance and assurance • Vulnerability Management	• Vulnerabilities in the supply chain should be addressed • Cybersecurity processes automation (smart decisions)

The following issues were also identified in the brainstorming session:

- **Job activities**
  - Experts highlighted the need for cybersecurity architects. This was one of the additions to ESCO suggested by ASSETS+'s cybersecurity team.
  - There is a need to intensify awareness of cyber risks at the top level management of organizations. Besides CISOs, a Chief Product Security Officer is a necessary role. In addition, it is essential to gain integration of skills from enterprise security and product security areas, as both overlap to some extent. Thus, it is important to gain these skills for managerial positions.
  - There is a need for cybersecurity specialists among the operators in the (battle)field (e.g., ships, crews). At least, basic level and closely related to the product they handle.
  - Cybersecurity involves several disciplines, and cybersecurity skills should be integrated into all of them. Traditional domains, like aviation, are getting more and more exposed to cybersecurity. Cybersecurity professionals should know systems and products certification.
  - There is a need to improve security in the software development and deployment process: SecDevOps.
  - It is advisable to count with adversarial skills. Particularly skills on how to attack when the organisation is under attack. However, this was excluded from the scope of ASSETS+
  - It is essential to fully understand and have the ability to use open-source and community developed components such as Docker or Kubernetes.
- **Education and training**
  - Agile courses should keep up with evolving technologies. Short courses (e.g., 6 months course is not acceptable) and lifelong learning activities should be developed.

- Gamification will be the way of training, but with real case exercises, not prepared ad-hoc. In this regard, cyber ranges are excellent approaches to deal with this issue, but the problem is to keep exercises up to date. ASSETS+ had already pointed out cyber ranges as a promising technology.
- Cybersecurity awareness across the whole organization is a relevant issue. There are no specific techniques or training, but there should be.
- The industry should be involved in education. Academic and industrial points of view are essential for the learning process.
- There is a shortage of incident responders.

It is useful to focus on shorter courses, also virtual ones, instead of heavy long-lasting ones.

- **Connectivity and IoT**: Need to analyze also (Industrial) Internet of Things.
- **Data Analytics and AI:** Also useful to add the 'learning by doing' or On the Job Training
- **Mixed Reality**: Need to add Augmented Reality in some plants, and the trend is to increase and facilitate people's using it, as well as Virtual Reality, for which we'll need training.
- **Embedded Security**: security of decentralized edge devices must be considered
- **Secure Software Development**: need of skilling to use/develop tools like security code analysers to be added

2.3 The impact of Artificial Intelligence in Defence areas (Air, Naval, Space, Sea, Cyberspace and Factory)

This brainstorming session involved 3 technical experts from 3 different companies of the ASSETs+ Consortium.

They generated 35 different ideas in the 3 parts within the brainstorming session. The parts were dedicated to technologies and applications, job activities, education and training. The virtual boards of each part are reported in the Figures 9, 10 and 11.

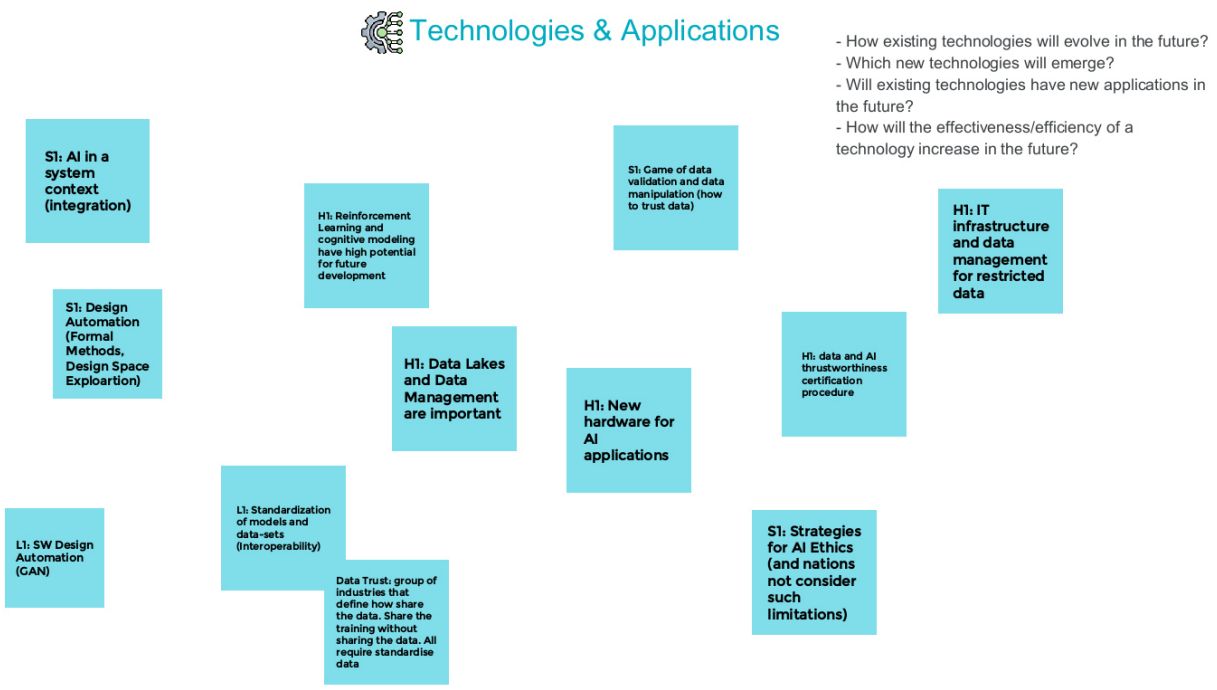

Figure 8 - Board for the technologies and application part in the brainstorming session on "The impact of Artificial Intelligence in Defence areas (Air, Naval, Space, Sea, Cyberspace and Factory)".

Figure 9 - Board for the job activities part in the brainstorming session on "The impact of Artificial Intelligence in Defence areas (Air, Naval, Space, Sea, Cyberspace and Factory)".

Figure 10 - Board for the education and training part in the brainstorming session on "The impact of Artificial Intelligence in Defence areas (Air, Naval, Space, Sea, Cyberspace and Factory)".

The experts' ideas are compared with the technologies and applications identified in the data-driven analysis with the purpose to detect the missing elements.

The Table 3 summarises the list of identified technology, related technologies from the technology roadmap, and explanations/comments. Note that the colours refer to the following:

- **Red:** technology not included in the latest version of the technology roadmap report.
- **Orange:** relevant technology, but already exists as a combination of technologies or in a more generic terminology.
- **Green:** technology already included in the technology roadmap report.
- **Blue:** not technology, but needs.

Table 3 - Table of technologies observations derived from the brainstorming session on " The impact of Artificial Intelligence in Defence areas (Air, Naval, Space, Sea, Cyberspace and Factory)".

Technology	Corresponding technology current roadmap (if any)	Comment/Specific application
Artificial Intelligence in a system context (integration)	Artificial Intelligence	Combining different AI methods
Design Automation (Formal Methods, Design Space Exploration)	Artificial Intelligence Automation	Automation and AI in designing process

Technology	Corresponding technology current roadmap (if any)	Comment/Specific application
Reinforcement learning and cognitive modelling	Reinforcement learning Human Machine Interaction	Applied in decision making process
Software Design Automation Generative Adversarial Network (GAN)	Machine learning Neural networks	Creating a system that will develop code from requirement or from a description of the expected behavior
Data Lakes and Data Management	Data Management	Data Management for the purpose of certification
New hardware for AI applications	Field Programmable Gate Array, (FPGA)	Certificated hardware for the critical infrastructure systems. For example, a dedicated hardware that support the autonomous drive systems ***Note:*** *This is not a technology as it looks more like a need for a new technology*
Data testing Data validation	Data Management	Game on data validation and data manipulation Cyberwarfare
Data and AI trustworthiness certification procedure	Artificial Intelligence Data Management	Improve the explainability of the AI algorithms ***Note:*** *This is not a technology as it looks more like a system of certification.*
Standardization of models and data-sets (Interoperability)	Interoperability	Standardize models to test the performance between different models. Share the training without sharing the data. All require standardize data. ***Note:*** *This is not a technology as it looks more like a skills/job function. Standardization is needed to ensure interoperability.*
Strategies for AI Ethics	Artificial Intelligence	How to deal with different approaches to AI ethics in the world? ***Note:*** *This is not a technology as it looks more like an approach.*
IT infrastructure and data management for restricted data	Data Management	How to deal with the restricted data? ***Note:*** *This is not a technology as it looks more like a need for a new technology.*

Based on the analysis of the abovementioned technologies, the following technologies were identified:

- **Cognitive modelling:** this is loosely related to Human Machine Interaction; can be used to simulate or predict human behaviour or performance on tasks similar to the ones modelled and improve human-computer interaction,
- **Generative Adversarial Network:** two models are trained simultaneously,
- **Data Lakes:** a system or repository of data stored in its natural/raw format.

In addition, other technologies that are relevant were mentioned and these are: **Data testing** and **Data validation**. They are connected with Data Management.

Additionally, a need for new technologies was underlined: the technologies **for certificated hardware for the critical infrastructure systems and to deal with restricted data.**

Moreover, it was identified that new strategies are also needed **to deal with different approaches to AI ethics in the world, for standardization of models and data-sets.**

Elements to be considered in the definition of Roadmaps for Technologies, Job activities and Education and Training:

It is recommended to consider, some of the work lines US DARPA (link) is currently through, like:

- ***High Performance AI or Quantum AI****: Computer performance increases over the last decade have enabled the success of machine learning, in combination with large data sets, and software libraries. More performance at lower electrical power is essential to allow both data center and tactical deployments. Analogue processing of AI algorithms has been shown to achieve 1000x speedup and 1000x energy efficiency over state-of-the-art digital processors. Quantum AI or the training of models on quantum computers poses a serious threat at the military level, as training models that would take thousands of years in hours would mean tactical supremacy in all systems with AI. Another line of work is to address the current inefficiency of machine learning by investigating methods to drastically reduce the need for labelled training data.*
- ***Robust AI:*** *AI technologies have demonstrated great value to missions as diverse as space-based imagery analysis, cyberattack warning, supply chain logistics and analysis of microbiologic systems. At the same time, the failure modes of AI technologies are poorly understood. The success is essential for to deploy AI technologies, particularly to the tactical edge, where reliable performance is required.*
- ***Adversarial AI:*** *The most powerful AI tool today is machine learning (ML). ML systems can be easily duped by changes to inputs that would never fool a human. The data used to train such systems can be corrupted. And, the software itself is vulnerable to cyber attack. These areas, and more, must be addressed at scale as more AI-enabled systems are operationally deployed.*

Additional elements:

- The importance of multidisciplinary skills and qualifications over specialised ones
- Availability of online self-learning platforms, with official qualifications (upskilling / reskilling for technicians to implement, collaborate or benefit from AI projects)
- There is definitely a need to further precise the skills around Cyber Security Architecture. It is vital that this is considered, as only looking at SecDevOps does not cover the full picture, as it is only looking at "Security by Design '' on application/ platform level. However, especially in Defence, we will equally have to look at how all those applications/ platforms are architected in most secured way. The way it is mentioned in the doc is too top level for me and would need more attention.

- Another key point is Industrial Cyber Security, meaning how to secure machine and device connection/ networks.

The following issues were also identified in the brainstorming session:

- **Job activities**
  - we distinguish the following relevant job activities:
    - Human-machine interaction.
    - Teach AI know-how.
    - Data analysis and statistic properties.
    - Monitoring and controlling.
    - Building awareness of broader context.
    - Building awareness of the potential and threats of artificial intelligence.
    - Collaboration with end-customers to collect product performance data.
    - Critical analysis on the results provided by AI - understanding the results received from an automatic analysis.
- **Education and training**
  - the following recommendation from industry experts concerning education and training – topics expected to be taught:
    - System engineering.
    - Data source and data assessment.
    - AI methods selection for specific cases.
    - Hybrid AI system.
    - Automatic analysis to support decision making.
    - Awareness of defence sector needs and differences between defence and other sectors' needs.
  - The experts mentioned several learning techniques:
    - You Tube online lectures – short knowledge interventions.
    - Learning across industries.
    - In-house trainings.

2. Re-elaboration of the results from brainstorming sessions

The comparison presented in the previous paragraph is the basis for the development of specific roadmaps that describe the evolution of the technological domains in the near future.

Those maps, presented in the following Figures 2 and 3, include:

- On the x axis, the timeline, it describes the maturity level of the technologies.
- On the y axis, the Defence-related applications, identified and mapped in the data-driven analysis as presented in the Annex 1 of this report.
- In the plot, the technologies.

The position of each technology is given by their level of maturity and their relevance within a given defence related application. That information, enriched with the valuable comments collected during the brainstorming sessions, allowed the WP1 team to cluster the technologies and provide the full picture of the current technological domains in such a complex panorama, as the Defence domain.

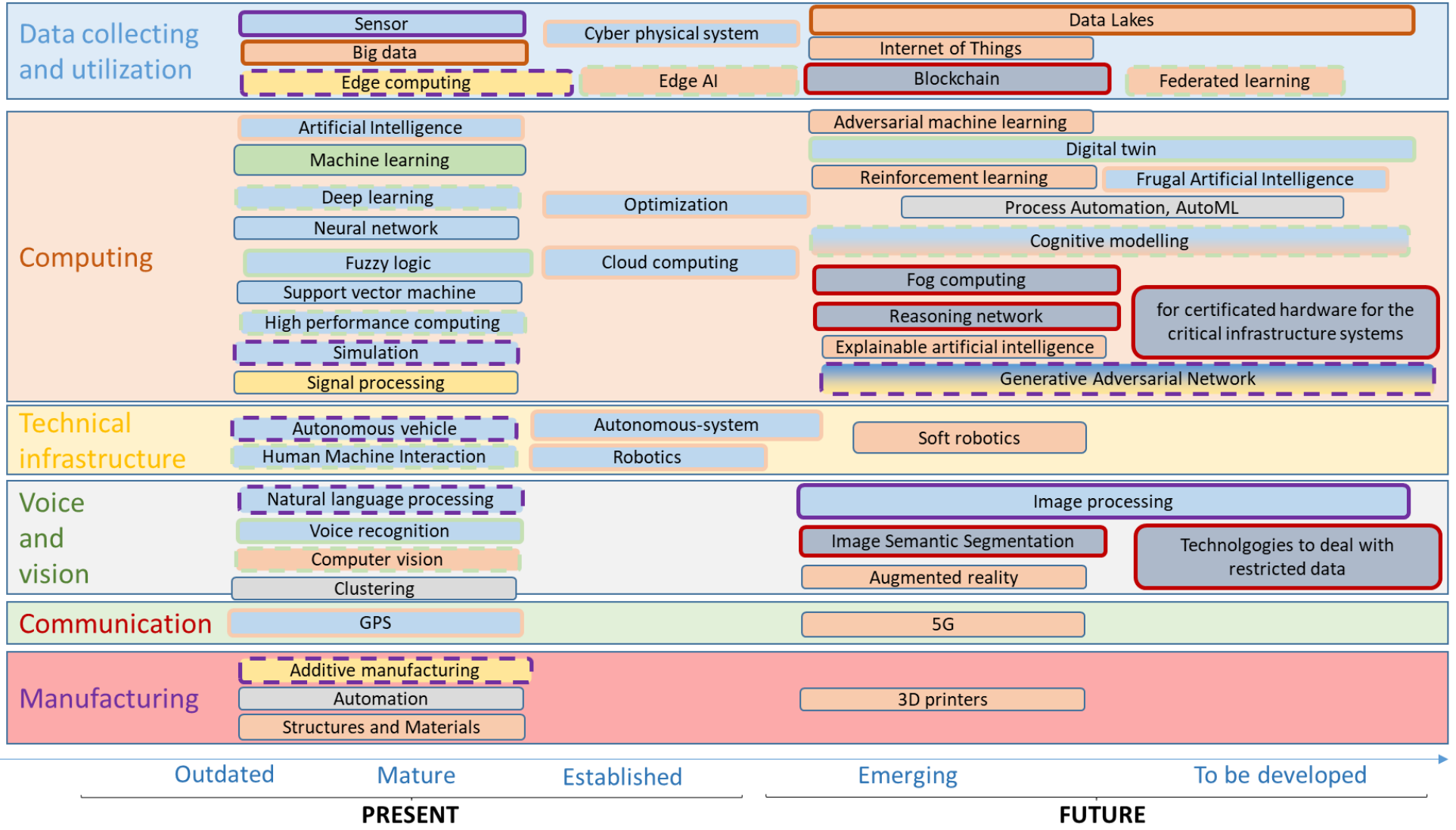

Figure 11 - Artificial Intelligence, Robotics, Autonomous Systems Technology and Applications Roadmap.

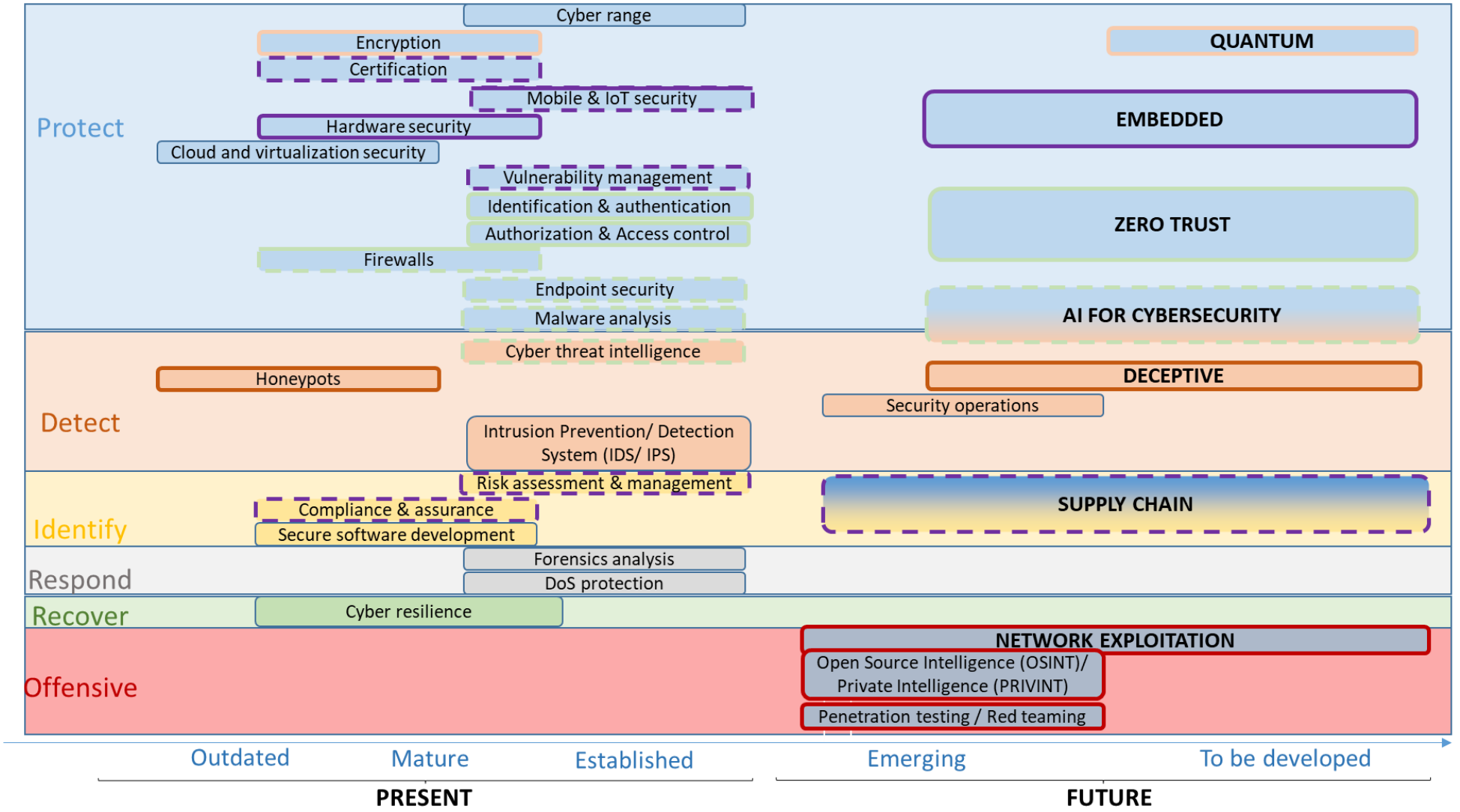

Figure 12 - Cybersecurity Technology and Applications Roadmap.