R1.4 - Skills and Job Profile Validation

Dissemination level: CO (confidential)

Grant Agreement Number:	**612678-EPP-1-2019-1-IT-EPPKA2-SSA-B**
Project acronym:	ASSETs+
Project full title:	Alliance for Strategic Skills addressing Emerging Technologies in Defence
WP number and tittle:	WP1 - Technology and Skills Analysis
Tittle of the deliverable:	Skills and Job Profile Validation
Deliverable number:	R1.4
Responsible partner:	Leonardo
Contributing partners / fellows:	AAU, AEROCAMPUS AQUITAINE, AIRBUS, CENSEC, EWF, HENSOLDT, NEXEYA, MADRID AEROSPACE, ELINGUA, NAVANTIA, ROLLS ROYCE, SAAB, SAFRAN, SEAUEROPE
Document's status	Final

Document's development track:

	Version of the document	Organisation	Name, Surname	Date
Drafted by:	V.1	LEONARDO	Massimo SCALVENZI	20/07/2021
Reviewed by:	V.2	AAU AEROCAMPUS AQUITAINE AIRBUS CENSEC EWF HENSOLDT NEXEYA MADRID AEROSPACE ELINGUA NAVANTIA ROLLS ROYCE SAAB SAFRAN SEAUEROPE	Soli OLOFSSON BAK Sandra PERNET Sonja MUELLER Klaus BOLVING Adelaide ALMEIDA Nathalie RIEUTORT Jerome SENARD Carlos ROMERO Miguel CAMACHO Eduardo GOMEZ Marting GARCIA Antoine FERAL Stefan ANDERSSON Sabrina GOTTLIEB Laura CARBONE	27/07/2021
Released by:	V.3 Final Version 1	Leonardo	Massimo SCALVENZI	29/07/2021
Drafted by:	V.4	LEONARDO	Massimo SCALVENZI	17/02/2022
Reviewed by:	V.5	AAU AEROCAMPUS AQUITAINE AIRBUS CENSEC EWF	Soli OLOFSSON BAK Sandra PERNET Sonja MUELLER Klaus BOLVING	22/02/2022

		HENSOLDT NEXEYA MADRID AEROSPACE ELINGUA NAVANTIA ROLLS ROYCE SAAB SAFRAN SEAUEROPE UNIPI	Adelaide ALMEIDA Nathalie RIEUTORT Jerome SENARD Carlos ROMERO Miguel CAMACHO Eduardo GOMEZ Martin GARCIA Antoine FERAL Stefan ANDERSSON Sabrina GOTTLIEB Laura CARBONE Irene SPADA	
Released by:	V.6 Final Version 2	Leonardo	Massimo SCALVENZI	25/02/2022
Released by:	V.7 Minor Updates	Leonardo	Massimo SCALVENZI	22/12/2022
Drafted by:	V.8	LEONARDO	Massimo SCALVENZI	23/02/2023
Reviewed by:	V.9	AEROCAMPUS AQUITAINE AIRBUS CENSEC EWF HENSOLDT MADRID AEROSPACE NAVANTIA ROLLS ROYCE SAAB SAFRAN SEAUEROPE UNIPI	Sandra PERNET Sonja MUELLER Klaus BOLVING Sara FERNANDES Nathalie RIEUTORT Carlos ROMERO Miguel CAMACHO Martin GARCIA Antoine FERAL Navid AZADI Anna MALM Jerome DE LA BROSSE Laura CARBONE Irene SPADA	27/02/2023
Released by:	V.10 Final Version 2	Leonardo	Massimo SCALVENZI	28/02/2023

** Note from the Project coordinator: draft document is expected from the task leader and can involve other partners; the review of the document is performed by the task fellows, including the WP leader.*

Index

Table index

1. Introduction

The ASSETs+ project 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**;
- **C4ISTAR**;
- **Cyber Security**.

As a summary of the activity, the first edition regards the validation of industrial partners for the data driven analysis. The second edition of this task concerns the validation of industrial partners for the brainstorming sessions. Those brainstorming sessions were not planned in the initial proposal, and they had a twofold objective:

- first to identify lacks in the data driven analysis (especially weak signals)
- and then to integrate new stimuli for the future of the research.

As the reader will find out, industrial experts in the first edition of the validation provided a greater and much more detailed feedback rather than in the second edition. However, this is an expected result. Actually, the brainstorming sessions improved a lot the data driven outcomes because during the sessions, the industrial experts shared their visions, feedback, suggestions and recommendations. All the information were included in the new version of the report R1.2 and R1.3 in a large process of data integration, which was complemented also by additional in-depth analyses on roadmapping. Therefore, the second edition of the validation registered a lack of recommendations and changes, as those have been collected “live” during the brainstorming sessions.

The final validation concerns the final version of the results; therefore, the goal will be to verify the clear, consistent, comprehensive, well organised, and coherent presentation of the results.

The **second iteration** of T1.4 has been then focused on dedicated to the review of the brainstorming sessions that involved the industrial partners of ASSETs+, aimed at the identification of recommendations concerning education and training for the Technologies and Applications road maps in the three domains.

The **first iteration** of the task did a first validation from the industrial partners of results coming from T1.2 and T.13 in order to ensure the alignment between emerging skills needs and labour market demand within the three domains.

The validation consisted of:

1. **Evaluating the methodologies** followed in T1.2 and T.3 regarding three domains, identifying some areas improvement, where possible.
2. **Scoring** the completeness of Technologies and Applications identified in T1.2 for the three domains, identifying some gaps and proposing additional sources of information, where possible.
3. **Scoring** the completeness of Skills documented in T1.3 for the three domains, identifying some gaps and proposing additional sources of information, where possible.

While conducting the validation of T1.2 and T1.3 it was decided to ask to the industrial partners to validate also the outcome of T1.1.

2. Final Validation Outcome

The Final Validation has been based on what is currently published on the website: https://assets-plus.eu/results/defence-technologies-roadmap-skills-blueprint/.

Figure 1 - Job Profiles, Technologies & Skills Roadmap

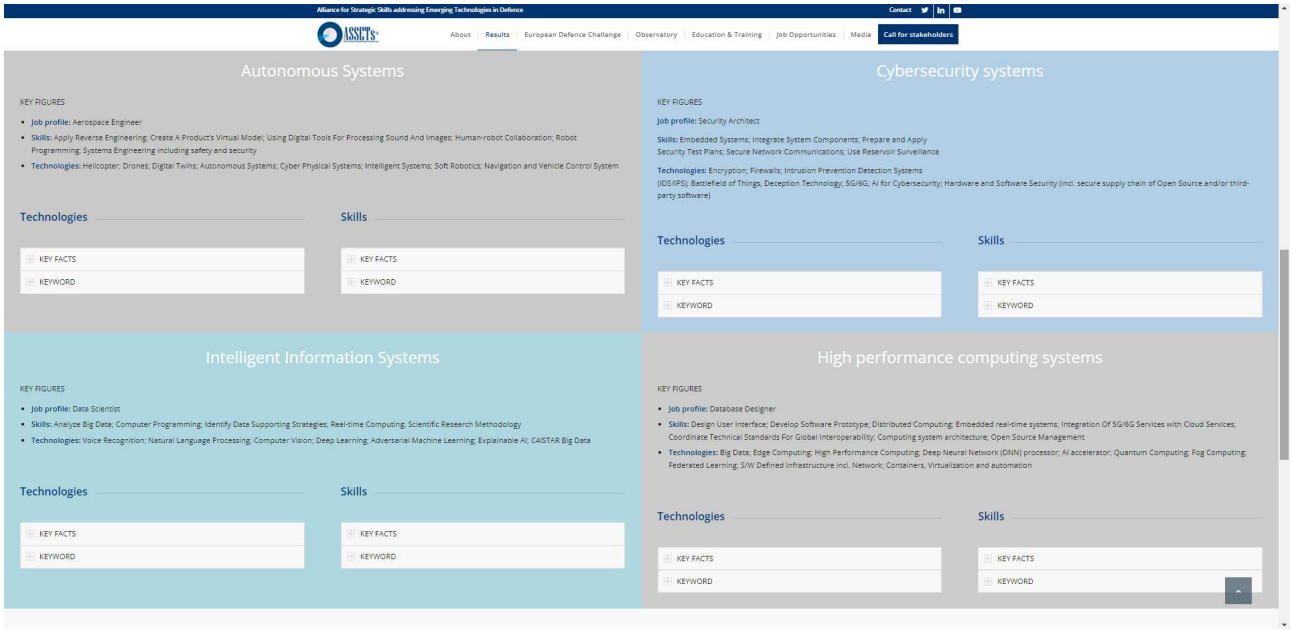

Figure 2 - Description of the capabilities areas

The final validation has been conducted by Task Fellows according to these Evaluation Elements to be considered:

- **Content coherence**: if the emerging technologies and skills are in line with the needs defined;
- **Content completeness**: if all the important information from the automated analysis, the brainstorming sessions and the various validation steps have been taken into account;
- **Presentation clarity**: if the results are presented in a clear way and with an appropriate language;
- **Results structure**: if the contents are easy to be browsed, between web page, main report and attachments;
- **Results coherence**: if the documents are all presented in the same way in terms of style and format.

In the evaluation the following grades have been taken into account:

- **Accepted**: Result fully validated
- **Minor concern**: the different elements are generally ok but some can be improved, giving hints on what and how to modify
- **Major concern**: there are many elements to be better described, what has to be modified and why

2.1 Results of Final Validation

The Task Fellows defined that **all the Evaluation Elements are considered Accepted**, and in the specific Content Coherence, Content Completeness and Presentation Clarity had a level of acceptance of 90%, while Results Structure and Results Coherence have reached a 100% of acceptance. In the following, some minor remarks are described (each highlighted only by one Task Fellow):

- **Content coherence**:
  - Cybersecurity: TEACH computer science - teach maybe not the right wording, more on investigate or develop;
  - Intelligent Information System: “open source management” to be reassessed – maybe not a priority;
  - The job profiles are very specific, for example Aerospace Engineer is too narrow as a job profile, preferably would for example System Engineer be applied
- **Content completeness**:
  - The job profiles are very specific, for example Aerospace Engineer is too narrow as a job profile, preferably would for example System Engineer be applied
- **Presentation clarity**:
  - The approach may be reversed moving to the list of competences/skills linked then to the 4 job profiles
- **Results structure**: none
- **Results coherence**: none

3. Second Iteration Outcome

3.1 Approach to perform the analysis for education and training for the Technologies and Applications roadmaps

With the aim to define the Job Activities and the Education and Training needed to support the roadmaps to look forward in the C4AID (Command, Control, Communication, Cyber Security, Artificial Intelligence, Defence) framework, it has been decided to create a matrix including the 4 Technologies and the 6 Defence Areas:

		Defence Areas					
		Factory	Land	Sea	Air	Space	Cyberspace
Technologies	Artificial Intelligence						
	Cybersecurity						
	Robot						
	Autonomous Systems						

Figure 3 – Brainstorming Sessions

As partners of T1.4, Industrial Partners were requested to define the most relevant intersections in the above matrix and to appoint experts that would eventually support the Brainstorming Sessions.

3.2 The roadmaps selected for the Brainstorming Sessions

After having received all the contributions, at WP1 level, the most relevant areas have been selected considering a more punctual approach vs a technology-oriented one or a defence area-oriented one, bringing to the following choice for the Brainstorming Sessions:

1. Cybersecurity for Defence areas (Air, Naval, Space, Sea, Cyberspace and Factory)
2. Artificial Intelligence, robotics, autonomous systems for the Sea domain
3. Artificial Intelligence for Defence areas (Air, Naval, Space, Sea, Cyberspace and Factory)

3.3 Synthesis Outcome of the Brainstorming Sessions performed

The Brainstorming Sessions have been conducted with the support of WP1 leadership, in a structured and mostly standard approach outlining, for each technology in the Technology area, the corresponding Technologies and Applications roadmaps and their inclusion in the latest Technologies and Applications roadmap report.

The objective of the Sessions was to define the most relevant Technologies and Applications Roadmaps, the related Job Activities Roadmap and the recommendations for Education and Training Roadmap.

3.3.1 Outcome of the Session dedicated to "Cybersecurity for Defence areas (Air, Naval, Space, Sea, Cyberspace and Factory)"

Current **Technologies and Applications Roadmap** has been presented to industrial partners in various ASSETs+ contexts, such as the Industrial Meetings and the WP1 Progress Meetings. The approach and structure for this Roadmap has been considered as an example to be considered in the other domains.

Industrial Partners have no specific comments to improve what has been done so far, since there are no missing elements in what has been considered in the first iteration.

Job Activities Roadmap

- Experts highlighted the need for cybersecurity architects with systemic view on security. 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. Thus, it is important to gain these skills and insights in managerial positions.
- There is a need for cybersecurity specialist s among the operators in the (battle)field (e.g., ships, crews) supported by cybersecurity automation – speed is of essence. 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 domain s, like aviation are getting more and more exposed to cybersecurity . Cybersecurity professionals should know system s and product s certification.
- There is a need to improve security in the software development (supply chain) and deployment process: SecDevOps.
- It is advisable to count with adversarial skills . Particularly skills on how to deceive or attack when the organisation is under attack. This aspect needs further discussions.
- It is essential to fully understand and have the ability to use open source and community developed components such as Docker or Kubernetes including the whole supply chain.

Education and Training Roadmap

- 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 and understanding of the threats 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 point s of view are essential for the learning process.
- There is a shortage of incident responders

3.3.2 Outcome of the Session dedicated to "Artificial Intelligence, robotics, autonomous systems for the Sea domain"

Technologies and Applications Roadmap

Based on the analysis of the results of the brainstorming sessions, 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 Technologies and Applications 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 Technologies and Applications roadmap. We cite among others:

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

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.

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.

3.3.3 Outcome of the Session dedicated to "Artificial Intelligence for Defence areas (Air, Naval, Space, Sea, Cyberspace and Factory)"

Technologies and Applications Roadmap

Based on the analysis the results of the brainstorming sessions, 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,
- 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.

Job Activities Roadmap

Based on the outcome of the brainstorming activities, we distinguish the following 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 Roadmap

The brainstorming resulted in 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.

Mentioned learning techniques:

- You Tube on line lectures – short knowledge interventions.
- Learning across industries.

- In-house trainings.

3.4 Industrial Partners Review of the Brainstorming Sessions

Industrial partners provided few comments on the three brainstorming sessions carried out, and the comments may bring further improvements to the sessions outcome.

3.4.1 Outcome of the Session dedicated to "Cybersecurity"

It is useful to focus on shorter courses, also virtual ones, instead of heavy long-lasting ones. Other important comments are:

- **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

3.4.2 Outcome of the Session dedicated to "Artificial Intelligence, robotics, autonomous systems for the Sea domain"

Concerning technologies, it is reminded that Machine Learning should therefore be identified as a technology for this topic, also for big data.

It would be preferable to cluster the competences according to the model below, proposed by Airbus.

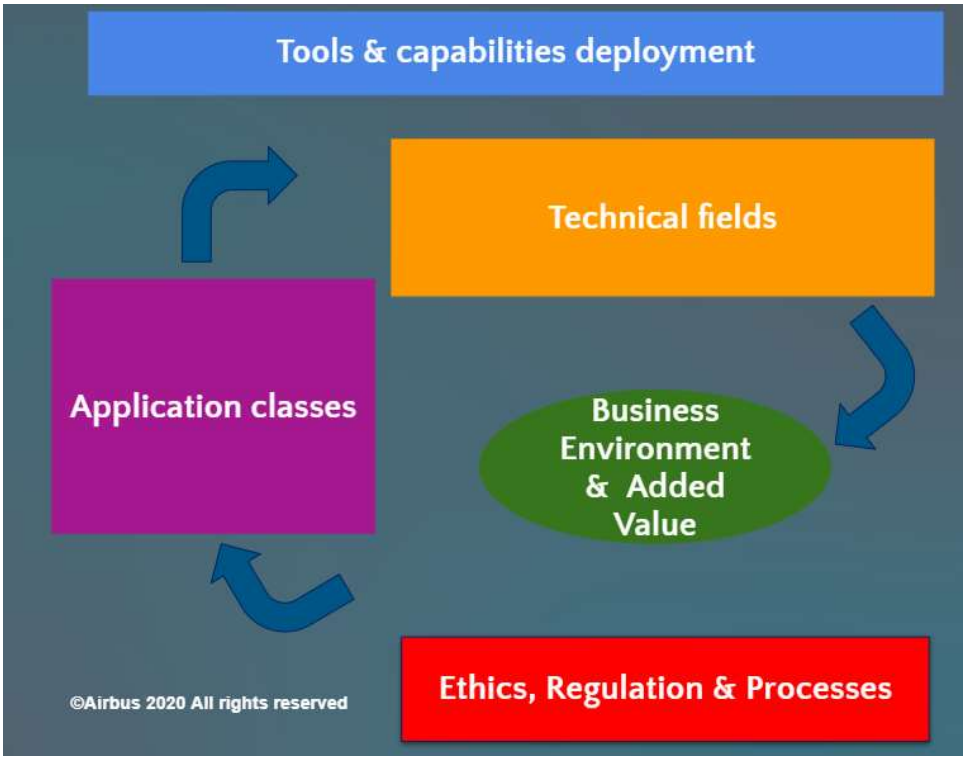

Figure 4 – Proposed Clusterization

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 professsionals. 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

3.4.3 Outcome of the Session dedicated to "Artificial Intelligence for Defence areas (Air, Naval, Space, Sea, Cyberspace and Factory)"

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 is currently through, like[1]:

- ***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.*

[1] From: https://www.darpa.mil/work-with-us/ai-next-campaign#:~:text=Adversarial%20AI%3A%20The%20most%20powerful%20AI%20tool%20today,the%20software%20itself%20is%20vulnerable%20to%20cyber%20attack.

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.

3.5. Conclusions of Second Iteration

Industrial partners generally found the outcome of the brainstorming sessions very useful, with the need of few adjustments and the addition of details, but the output of the brainstorming sessions is finally looking at the future of the ASSETS domains and to C4AID Framework.

It is also important that continuous development of technology roadmaps, analysis of impact on jobs and education is part of the outcome of ASSETs+. Technologies, applications and needs will continuously evolve and therefore education will need to evolve too.

4. First Iteration Outcome

4.1 Evaluation Questionnaire

The “Evaluation Questionnaire” has been validated by WP1 leaders and has been submitted to all Industrial partners of T1.4 and discussed in few conference calls prior to the results collection.

The template of the “Evaluation Questionnaire” is available in Appendix 1.

The list of Questions is the following:

Question # 01: Understandability of the methodology explained in document "R1.1 Strategy Specification"

Question # 02: Level of agreement of the concept of "Level of Maturity" explained in document "R1.2 Technology Roadmap"

Question # 03: Level of agreement of the concept of "Level of Abstraction" explained in document "R1.2 Technology Roadmap”

Question # 04: Completeness of the list of Applications considered in document "R1.2 Technology Roadmap" and related DB

Question # 05: Completeness of the list of Technologies considered in document "R1.2 Technology Roadmap" and related DB

Question # 06: Level of agreement of the methodology used for Skills classification in document "R1.3 Skills blueprint"

Question # 07: Completeness of the list of Skills considered in document "R1.3 Skills blueprint" and related DB

For each of the questions, the Partners could choose among 5 level of agreement, evaluated from 1 to 5, where 5 represents the highest level of agreement possible

4.2 Results

This paragraph presents the results of validation in the three different domains:

- Robotics, AI & autonomous system;
- C4ISTAR;
- Cybersecurity.

The answers received for the three domains are the following:

Domain	Number of Answers Received
Robotics, artificial intelligence (AI) and autonomous-systems	**6**
C4ISTAR	**2**
Cyber Security	**1**

Table 1 – Number of Answers received per Domain.

The Table 2 shows the average evaluation given by T1.4 Partners about the questions related to the three domains.

Domain	Question #1	Question #2	Question #3	Question #4	Question #5	Question #6	Question #7
Robotics, artificial intelligence (AI) and autonomous-systems	4,2	4	3,5	3,7	4,0	4,0	4,2
C4ISTAR	4,5	4,0	4,0	3,0	3,5	4,5	4,0
Cyber Security	5,0	5,0	5,0	4,0	4,0	5,0	5,0
Overall	**4,4**	**4,1**	**3,8**	**3,5**	**3,9**	**4,3**	**4,5**

Table 2 – Quantitative Evaluations per each Domain.

It is worth noting that it is difficult to derive final conclusions also because only few clarifications about gaps and areas of improvements have been submitted by the partners, but still some analysis are possible:

- General good evaluation about "R1.1 Strategy Specification" and for the completeness of the list of skills of "R1.3 Skills blueprint" and for the methodology used for Skills classification in "R1.3 Skills blueprint"
- Possible improvement are envisaged for the concept of “Level of Abstraction” and for the completeness of “List of applications” and “List of Technologies” in “R1.2 Technology Roadmap”; mostly for the domains Robotics, AI & autonomous system and C4ISTAR.

4.3 Additional comments received

a) Concerning the list of skills for the domain Robotics, AI & autonomous system:
   - The methodology is fine but from time to time Industry might be reluctant to adopt it systematically since it could be a little outdated (i.e. too rigid for the fast change of the modern world). The only potential change we may suggest (but it may be too complex for the market as a whole) is:
     i. To allow for greater flexibility a less rigid framework (or no framework at all) may be considered. Many organisations are now moving to a ‘skills cloud & talent marketplace’ approach – where people, training, projects & job roles are all

'tagged' (digitally) with the relevant skills. Each item can be tagged/untagged readily at any time from an over-arching 'skills cloud' (database). This does not require a complete re-work of the framework. This would, however, require investment in a system to manage such approach.

b) Concerning the domain C4ISTAR:

- **Question 1:**
  i. Acronyms: In C4ISTAR domain (and like other domains), acronyms have a strong meaning and we used many of them like IFF, SIGINT, ESM, ISR, AIS, INS, IMU, GPS, GNSS systems in many documents and papers. How does this survey consider these acronyms? How do you merge terms with the same meanings like SIGINT and "signal intelligence"?
  ii. Level of abstraction: Mixing of different levels of abstraction, from "low" to "high", looks problematic. It is very likely that technology with "high" (and some "medium") level of abstraction can overlap multiple domains or multiple applications, better than "low" one. Moreover, some "low" technologies are included into "high" technologies. It could be interesting to include a step into the methodology where "low" abstract terms are gathered with "high" abstract terms to create technology families. Thereafter, it may have more sense to compare relevance scores between technology families. A family should have more weight due to occurrences of all its "children" terms. Even if a term belongs to several families, it gives its score to reinforce its families. For example, "antenna" technology has 2 families:
     1. Tech Family "sensor" = {sensor, radar, antenna},
     2. Tech Family "communication system" = {communication system, router, server, gateway, receiver, antenna}
  iii. Application identification: About application identification, C4ISTAR seems a particular exception in comparison with Cyber, AI and autonomous system. C4ISTAR acronym is itself the summary of the eight main applications in this domain (see Question #04).

- **Question 2:**
  i. Cybersecurity should be qualified as "mature" technology (Instead of "Emerging", it is not starting to attract researchers and industries, for example Crypto Computers are common military embedded equipment).
  ii. If "Outdated" technologies mean "technologies that were relevant in the past but are now replaced with other technologies", then what technologies have replaced "radar", "sensor", "Internet", "Ethernet", "Linux" ? They look like "established" technologies nowadays. And if these technologies are finally outdated why the §4.2.3 in R1.2 concludes: "The relevance matrix registers the highest score for the combination of the following technologies: internet, information system, vehicles, aerial, interfaces, mobile, sensor, software;. Therefore, those are the first topics to address in designing the educational programmes".
  iii. Why educational programmes should be designed with outdated technology, instead of mature or established technology?

- **Question 3:**

i. Antennas, Cameras and radar should have the same level of abstraction.
ii. "Interfaces" is not a low level of abstraction; it is a large set of technologies and concepts. Interfaces are present in all technical domains like human-machine interface, mechanical/electrical/software/hardware interfaces, system/equipment/component interfaces. As an example, "USB" could be a low-level abstraction of "Interface" concept.
iii. Technology families could be easier to manage the level mix. For example:
    1. Tech Family "data analytics" = {data analytics, machine learning, data mining, neural networks, fuzzy logic}
    2. Tech Family "vehicle" = {vehicle, helicopter, drone, aircraft, ship}
    3. Tech Family "sensor" = {sensor, radar, antenna},
    4. Tech Family "communication system" = {communication system, router, server, gateway, receiver, antenna}

- **Question 4:**
    i. C4ISTAR is already a summary of the eight main applications to map with technologies:
        1. Command
        2. Control
        3. Communications
        4. Computers (means "Data Processing")
        5. Military Intelligence
        6. Surveillance
        7. Target Acquisition
        8. Reconnaissance
    ii. The conclusion of §4.2.3 of R1.2 document is surprising: "programming" is among the six most relevant applications related to a C4ISTAR system. "Programming" is a design activity, required to develop a C4ISTAR system. Nevertheless, "Programming" is not relevant as operational application (like surveillance, reconnaissance, intelligence). It could be seen more as a technical skill.
    iii. In R1.1, the paragraph "2.1.3 Identify applications" defines clearly the idea of operational applications: "Application is a cornerstone concept for the ASSETs+ project, since technological systems support users in various activities during defence operations and missions to reach the defined goal thanks to some specific characteristics of the systems themselves.

- **Question 5:**
    i. We propose to add following technologies into Tech classification C4ISTAR:
        1. Geographical information system (GIS)
        2. Data link equipment
        3. Optronic system
        4. Spectrum analysis
        5. High Performance Computing (HPC)
        6. Identification system
        7. Transponder

8. Interrogator
9. Direction finder
10. Electronic countermeasure
11. Electronic self-protection system (EP)
12. Data recorder
13. Positioning system

ii. We propose to remove “Software” as this word has several meanings in papers. It is not only about technology but also a domain like “Electronic”. Like “Interface”, “Software” is a “big bag” of technologies: any non-hardware technology are software.

iii. Most of C4ISTAR systems are not connected or related to “Internet” technology. Why do text-mining tools collect this technology? Is it due to internet data sources?

iv. “Mobile” is a technology rarely used into C4ISTAR. “Mobile” is an ambiguous term used as noun or adjective. Perhaps papers refer to mobile targets. Does the Speech tagging filter mobile adjective? Alternatively, does speech tagging make errors? As an example from a HAL paper about C4ISTAR system: “An autonomous weapon may be mobile or stationary, it is distinguished from manned weapon system types by way of pre-loaded heuristics to undertake its C4ISTAR…”

v. We propose to remove “Linux”, “server”, “Internet”, ”Ethernet”, “Operating systems”, ”Interfaces” and “User interface”. A large amount of papers use these terms about software domain. Moreover, many standard educational programs in software engineering already include these software technologies. That is probably why they do not appear into tech classification tables for Cyber, AI and autonomous system domains.

- **Question 7:**

i. Skills prefix like “develop”, “use”, “maintain” is useful to distinguish between development skills, operation skills and system support skills. However, some development skills start with “use” prefix, perhaps a rewording could help:

1. “use software design patterns” => develop with software design patterns
2. “use interface description language” => develop with an interface description language
3. “use automatic programming” => develop with automatic programming

ii. What do you mean by “mine” planning software? C4ISTAR has nothing related to “mining” domain.

iii. Why are some skills restricted to a specific vehicle (“ship”) or equipment (“reservoir”)?

iv. Skills that are more general would be more relevant. For example:

1. conduct analysis of ~~ship~~ data
2. use ~~water~~ navigation devices
3. use ~~reservoir~~ surveillance devices
4. use ~~specific~~ data analysis software

4.4 Conclusions of First Iteration

The evaluations given by T1.4 Partners can be taken into account in the next revision of R1.2 and R1.3, maybe with a direct involvement of the T1.4 Partners during the drafting phase, with the aim of collecting many more comments than the ones received so far.

The proposed approach could also result, in the future, in a more important and deep contribution for the next revision of R1.4.