Deliverable R1.3
Skills Blueprint

Dissemination level: PU (public)

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

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 Technologies and Skills Analysis
Tittle of the deliverable:	Skills Blueprint
Deliverable number:	R1.3
Responsible partner:	UNIPI
Contributing partners / fellows:	UBX, PRZ, UCIII, AAU, FGB, UNISEVILLE
Document's status	final

Document's development track:

	Version of the document	Organisation	Name, Surname	Date
Drafted by:	V.1	(list all authors)* UNIPI AAU UBX PRZ UCIII UNISEVILLE	Vito Giordano Irene Spada Mohamed El Yafrani Peter Nielson Marie Raoul Johannes Van Der Pool Eric Grivel Dorota Stadinka Jose Maria de Fuentes Daniel Segovia Rafael Estepa Alonso Jaime Dominguez	March 2020
Reviewed by:	V.1	(list all reviewers)* UNIPI	Filippo Chiarello	December 2020
Released by:	V.2	(Task leader)* UNIPI	Filippo Chiarello	March 2020
Drafted by:	V.2	(list all authors)* UNIPI AAU UBX PRZ UCIII UNISEVILLE FGB	Irene Spada Mohamed El Yafrani Marie Raoul Eric Grivel Dorota Stadinka Jose Maria de Fuentes Daniel Segovia Lorena Gonzales Rafael Estepa Alonso Jaime Dominguez Francisca Tena Tena	April 2021
Reviewed by:	V.2	(list all reviewers)* UNIPI	Filippo Chiarello Gualtiero Fantoni	April 2021
Released by:	V.2	(Task leader)* UNIPI	Filippo Chiarello	April 2021
Drafted by:	V.3	(list all reviewers)* UNIPI	Irene Spada	September 2022
Reviewed by:	V.2	(list all reviewers)* UCIII	Jose Maria de Fuentes	October 2022
Released by:	V.3	(Task leader)* UNIPI	Irene Spada	December 2022
Reviewed and Released by:	v.4	(Task leader)* UNIPI	Irene Spada	December 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.*

Table of Contents

List of tables and figures

Tables

Figures

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:

the **common** parts are coloured in **blue**,
while the **different** pieces are in **black**.

1. Introduction

The ASSETS+ project aims at creating a strategy to upskill and reskill the Defence Human Resources supply chain (students and professionals). The technological focus of the project is on Robotics, Autonomous Systems, AI, Cybersecurity, and C4ISTAR and to skills and job profiles linked to these fields. The study of the relation between technology, work and education is challenging in general, but is even harder nowadays in a sector like Defence, where the innovation is always at the frontier and where information (both R&D and HR related) is rarely shared by companies.

This document belongs to the Work Package WP1, the first WP of ASSETs+ project, that feeds with information the rest of WPs. WP1, named *Technology and skill analysis*, aims at mixing automated tools and human expertise coming from ASSETs+ industries and Universities to understand and communicate the complex relations that exists between technologies, skills and job profiles in the defence sector. The use of qualitative and quantitative methods makes it possible to handle the complexity of such tasks. Indeed, big data analysis of technical and scientific documentation helps to understand the skills that are necessary to properly exploit the emerging technologies in Defence; and those skills will be included in the design and update of education & training programmes for the re/up-skilling of the current and future workforce. We also look at these technological domains in a holistic and future-oriented way, harnessing the expertise of our partners. All the output are in fact the results of a strong cooperation between academic and industrial partners of ASSETs+. Also, the results are independently validated by industrial experts to align them with the needs of the sector. Moreover, the activities are repeated annually to monitor relevant skills and to spot the emerging ones.

The technological areas on which ASSETs+ is focused (**Robotics, artificial intelligence (AI) and autonomous-systems**, **C4ISTAR** and **Cybersecurity**) give to the whole project a wide view on the technological dynamics of Defence. Given the continuous evolution that we are facing in these areas, a clear understanding of their impact on the defence workforce is also relevant for preserving the European autonomy and sovereignty. Assuring that the defence workers of the future have the right skills concerning technologies such as drones, deep learning, or the cyber warfare, is a requirement for managing the challenges that European companies and institutions (defence related, but also civil) will need to face soon.

This document contains the results of the skills analysis of WP1, that can be synthetised in a technological roadmap. This roadmap must be intended as different form the typical roadmap that the reader may have encountered in his/her career. The aim is in fact to ease the understanding of how technologies can impact on the defence workforce, and how to guide the design of future define related courses (which is the goal of the project). Here, we focus on the results of the process, without focusing too much on

the methodological descriptions. The reader that is interested in the methodological details can read the scientific publications that derived from the executed analysis[1].

The rest of the document is structured as following: after a short summary of the current state of skills needs in the Defence sector (*Section 2*), in the S*ection 3* there are the description of rationale of the roadmap of technologies, skills, and job profiles and then 4 parts focusing on the 4 capabilities areas (defined in the roadmap). In each of those there is a descriptive overview of the area, then the emerging job profiles and skills are defined highlighting possible implication for the Defense sector, future trends, and synergies. Finally, the overall conclusion and the key insights for the education and training programs design are reported in *Section 4*.

[1] Chiarello, F., Fantoni, G., Hogarth, T., Giordano, V., Baltina, L., & Spada, I. (2021). Towards ESCO 4.0–Is the European classification of skills in line with Industry 4.0? A text mining approach. *Technological Forecasting and Social Change*, *173*, 121177.

Giordano, V., Chiarello, F., Melluso, N., Fantoni, G., & Bonaccorsi, A. (2021). Text and Dynamic Network Analysis for Measuring Technological Convergence: A Case Study on Defense Patent Data. *IEEE Transactions on Engineering Management*.

2. Current state

The evolution of technologies in various domain related to the defence industry is faster and more complex than in the past, especially for disruptive technology. Although this evolution is beneficial for the economic growth of the defence sector and is creating many opportunities for new types of jobs, it produced also needs for new skills to exploit the novel technologies.

Defense agencies face a growing challenge of effectively processing, exploiting, and disseminating C4ISTAR data from multiple, diverse senor platforms. Workers need analytical skills and cognitive capabilities to manage and process the data collected by the information systems, analysing, and evaluating information for the situational awareness. The advanced software demand of users with digital skills to write and submit instructions, specifications, sand programmes for computers and to exploit those systems. Therefore, the demand of STEM and ICT skills with references on multidisciplinary and technologies combination will more and more increase. Defence companies and institutions should be able to deal with illegal accesses to systems, thus having knowledge of authentication and identification technologies, as well as encryption and certification. Network protection is a key feature working in the defence sector, where endpoint security and IDS technologies become a priority. The combination and analysis of information is mandatory to identify threats, especially stealthier ones. Not just discovering threats is important, but also its prevention and mitigation, being useful risk assessment technologies. However, when attacks have occurred or there are suspicions that some malicious actions have happened, forensic analysis technologies could be helpful.

In addition, defence companies also seek transversal skills in their candidates. The so-called soft skills are associated with the ability to work in different conditions, communicate efficiently, and deal with people. Transversal skills are not directly linked to technical tasks but essential for a complete management. Some of these skills are critical thinking, conflict management, preparation and delivery of reports or complex problem solving, among others.

Therefore, nowadays it is necessary finding and applying different policies to increase the sustainability and the capacity of the European defence industry.

3. Defence Roadmap

The roadmap is presented in the form of a radar. Radar is an iconic Defence-related technology, that is used as detection system, and has been chosen for several reasons, below to facilitate the understating of our results.

First, the product lifecycle of the radar is an example of the traditional innovation paradigm in technological R&D. Indeed, radar was elaborated in secret for military purpose before and during World War II; then the civil uses were widely and vary, such as air and terrestrial traffic control, astronomy, anti-collision systems, ocean surveillance systems, meteorological monitoring; nowadays high-tech radar systems are fused with digital signal processing and advanced machine learning algorithm, to detect and extract relevant data also in contexts where the noise level is very high. In the context of digitalization this innovation paradigm is changing towards a shift civil-defence and/or a synchronous and synergic R&D process. Therefore, this contrast in the figurative framework aims to highlight this radical transformation.

Second, radar is a detection system and so their goal is to monitor a context and identify the relevant information within a given scope. Therefore, it is a technological representation of the goal of this document, aiming at exploring emerging trends in technologies within the technological domains of Robotics, Autonomous Systems, AI, Cybersecurity, and C4ISTAR and mapping their relations within the Defence-related applications.

Finally, it is the in line with the logo of the ASSETs+, ensuring the coherence with the goal of the project in general. Therefore, spot the trends in technologies and skills, translate them into concrete concepts as a basis for new education and training programs for the current and future workforce in Defence, leveraging on the expertise of the Consortium. Those two last elements recall the importance of human resources both in defining and applying policies, in fact the human brain is in the middle of the radar.

The radar is built around the Human Resources, one of the fundamental capabilities, together with technological means, for the European autonomy and sovereignty.

> *"The efforts needed to achieve the abovementioned goals are not limited to Research and Development [for the emerging technologies, ndr]. The EU must drastically improve its digital capacities. This includes the deployment of digital technologies, as well as the necessary digital skills for all the EU workforce. Europe must also develop key digital infrastructures, innovate and strengthen its industrial base, enhance its resilience and flexibility both in terms of technologies and supply chains.".*[2]

[2] https://digital-strategy.ec.europa.eu/en/activities/work-programmes-digital
https://ec.europa.eu/newsroom/repository/document/2021-46/C_2021_7914_1_EN_annexe_acte_autonome_cp_part1_v3_x3qnsqH6g4B4JabSGBy9UatCRc8_81099.pdf

The roadmap includes the most relevant *job profiles*, the most relevant *skills* for each job profiles and the most relevant *technologies,* emerging from the analysis done in WP1[3].

The technologies are positioned around the job profiles, considering the importance of a technology for a given job, and along the radial dimension, considering the level of maturity of a technology. In this way, the technologies, the skills, and the job profiles are distributed in four main areas, that describes the most relevant capabilities for the Defence sector with particular reference to the technological domains of Robotics, Autonomous Systems, AI, Cybersecurity, and C4ISTAR.

Those technological capabilities areas can be defined summarizing the functional purpose of the technologies and the related activities of the job profiles involved. The technological capabilities can be summarised with the generic words systems (sets of technologies, humans, methods, and processes). The areas are the following:

1. **Autonomous systems**
2. **Cybersecurity systems**
3. **Intelligent information systems**
4. **High performance computing systems**

As indicated by industrial experts during their consultations, those areas are the ones that are really relevant to the Defence field for the future.

The technological domains of Robotics, Autonomous Systems, AI, Cybersecurity, and C4ISTAR - in analysis in the ASSETs+ project – relate with the above-mentioned areas as follows:

- Robotics, Autonomous Systems and AI is linked to the broader field of Autonomous Systems, addressing devices and digital tools with a certain degree of autonomy in developing the assigned tasks.
- Cybersecurity is linked to Cybersecurity systems, inclusing both the hardware and software to ensure the protection of data and infrastructure.
- C4ISTAR is linked to the Intelligent Information System area for what concern the data and techniques for ensuring situational awareness and to the High-Performance Computing Systems area for what concern the technical infrastructure needed to manage and elaborate the data flow in the operations.

This broad definition allowed to highlights links and connections among the technological aspects (i.e., technologies and applications) and the intangible elements (i.e., skills and job profiles) of the domains.

[3] The radar is the result of a desk work based on re-elaboration and integration of the data-driven analysis (cfr. R1.2 - ANNEX 1 - Report of data driven analysis for the Defence Technology Roadmap), the comments gathered with the brainstorming sessions (cfr. R1.2 - ANNEX 2 - Report of brainstorming session with industrial experts), as well as the feedback received in the validation by industrial partners (performed in task T1.4). Therefore, it was not expected to reach a perfect match of the technologies, or skills, or job profiles with one annex or the other. Indeed, we find out that the mix of the contributions is more than just the sum of the collected information and leads to a more valuable result when considered as a whole. In addition, the annexes offer the evolution of the analysis since they have been developed in different times. Therefore, the annexes were added also with the aim of presenting the time evolution of the work from totally data driven to the final expert enriched version.

The job profiles, the skills and the technologies have been detected using a *blended, iterative* approach. This approach combines data-driven analysis and human expertise.

The data driven analysis of technical and scientific documents (patents, scientific publications, domain-related articles, industrial reports, and so on), with Natural Language Processing techniques, has been used to understand the emerging technologies in the above-mentioned area and the necessary skills to properly exploit them in Defence. The first part of the analysis was dedicated to the delineation of the technological domains and the skills needs, leveraging on a data-driven approach based on the analysis of technical and scientific documentations

The approach is based on the following main parts:

- Exploring each domain to identify the core *technologies*, their trends and classify them according to their maturity level.
- Identifying the *applications* of the technologies, to describe how these are adopted and applied in defence sector.
- Finding the *skills* that workers use in exploiting technologies and application during daily operations and missions
- Mapping the *job profile*s according to the identified skills.

The results of this first analysis are reported in the ANNEX 1, where the skills, and job profiles are identified and classified to provide a full picture of the actual landscape in the Defence sector and are the foundation for building up a comprehensive roadmap to guide the future development of Defence training courses.

The second part of the analysis is based on industrial experts' validation and the holistic and future-oriented brainstorming sessions with technical experts of the ASSETs+ Consortium. On the one hand, the industrial experts revised the report obtained with the data-driven analysis to ensure the completeness and the correctness of the results. On the other hand, the experts have been involved in online sessions to collected additional insight with reference to the future oriented time-framed relations of:

- *technologies and applications*: technologies are methods, systems and devices which are the result of scientific knowledge being used for practical purposes. Applications are the act of use something for a purpose;
- *job activities*: necessary activities to support the major job functions of a given job profile. They will be divided in activities related to the design/developments, use, maintenance, and knowledge of the technologies;
- *education and training*: the processes of transmitting skills and knowledge. They will be divided in events related to workers, postgraduates, graduates, and undergraduates.

The outcome of the sessions and the insights are reported in the ANNEX 2[4] and allowed us to acquire valuable information about the needs of the sector to properly contextualize the future trends.

[4] This is a twin annex for the Technologies Roadmap.

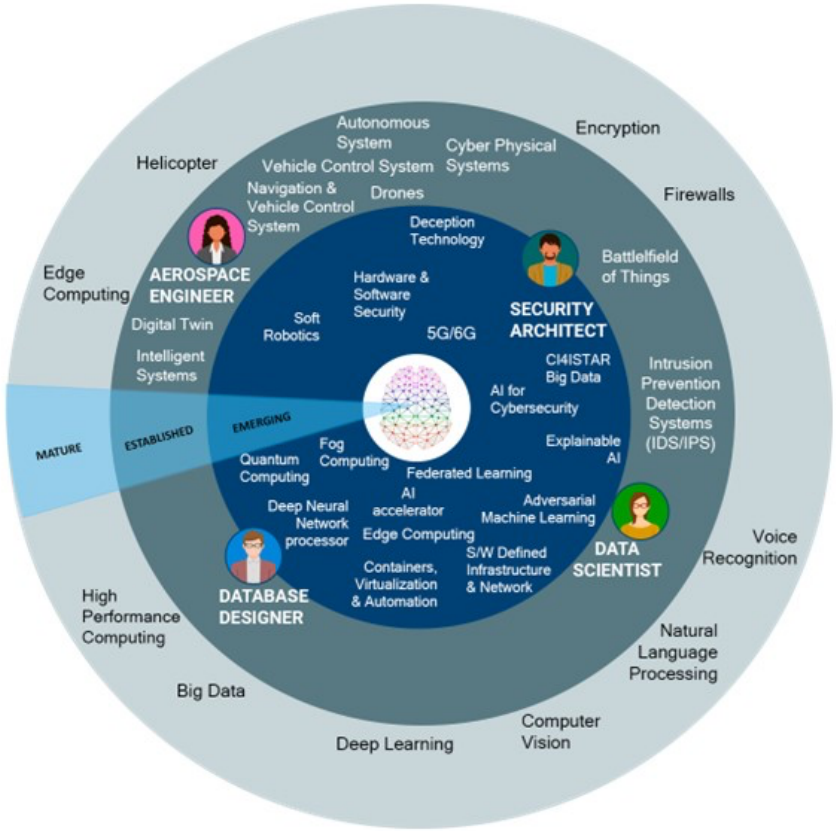
In this document the most relevant job profiles and skills are described, while a deeper analysis on the technologies and is available in the Technologies Roadmap.

CAPABILITY AREA: Autonomous Systems

- Aircraft Mechanics
- Apply Reverse Engineering
- Assemble Robots
- Control Systems
- Create a Product's Virtual Model
- Design Smart Grids
- Embedded Systems
- Guidance, Navigation and Control
- Human-Robot Collaboration
- Operate Drones in Civil Engineering
- Perform Aircraft Maintenance
- Perform Smart Grid Feasibility Study
- Robot Programming
- Set Up Automotive Robot
- Systems Engineering including safety and security
- Undertake Procedures to Meet Helicopter Flight Requirements
- Undertake Procedures to Meet UAV Flight Requirements
- Unmanned Air Systems
- Upgrade Firmware
- Using Digital Tools for Processing Sound and Images

CAPABILITY AREA: High Performance Computing Systems

- Analyse Big Data
- Artificial Neural Networks
- Computer Programming
- E-Learning Software Infrastructure
- Identify Data Supporting Strategies
- Real-time Computing
- Scientific Research Methodology
- Analyse Large-Scale Data in Healthcare
- Smart City Features



CAPABILITY AREA: Cybersecurity Systems

- Carry Out Research on Ground Systems
- Cyber Attack Counter-Measures
- Embedded Systems
- ICT Security Legislation
- Implement a Firewall
- Integrate System Components
- Manage Alarm System
- Manage Cloud Data and Storage
- Manage Keys for Data Protection
- Military Code
- Prepare and Apply Security Test Plans
- Secure Network Communications
- Teach Computer Science
- Use Reservoir Surveillance

CAPABILITY AREA: Intelligent Information Systems

- Artificial Neural Networks
- Computer Vision
- Computing system architecture
- Control Panel Components
- Coordinate Technical Standards for Global Interoperability
- Design User Interface
- Develop Software Prototype
- Distributed Computing
- Electrical Machines
- Embedded real-time systems
- Guide Learners in Using Assistive Technologies
- Integration Of 5G/6G Services with Cloud Services
- Make Electrical Calculations
- Natural Language Processing
- Open Source Management
- Power Engineering

Figure 1 - Job Profiles, Technologies & Skills Roadmap.

All the job profiles reported in the roadmap are mapped in the European classification of Skills, Competences, Occupations and Qualifications (ESCO).

An interesting insight is an apparent opposition between the two sides of the roadmap. On the left, two old-fashioned profiles have been detected as relevant, i.e., the *Aerospace Engineer* and the *Database Designer*. On the right, two fresh professions have been identified, i.e., the *Data Scientist* and the *Security Architect*. Indeed, all of them result to be **emerging** because to meet the challenges of the future and to make the best use of the potential of new technologies, both an adaptation of skills for the apparently traditional and well-established professions and the structuring of training activities for new professions are necessary.

The Table 1 reports a short description and the link to ESCO. ASSETs+ contributed to the process of review and integration of existing concepts, proposing a new occupational profile related to the cybersecurity area, namely the *security architect*, that has been added in the new version of the taxonomy, i.e., ESCO v1.1[5].

The four job profiles selected are considered essential for industry needs and they are described in a way that is wide enough to consider almost all the needs of other industries. Some better denominations can be envisaged, such as *Vehicle System Engineer* for the *Aerospace Engineer*, and *Secure Could-Edge Computing System Architect* for the *Database Designer*.

It this then fundamental to design and develop training path for the job profiles to fulfil needs of labour market.

Top job profiles in Defence		
Job title	**Job description**	**Link to ESCO taxonomy**
Aerospace Engineer	Develop, test, and oversee the manufacture of flight vehicles such as aircrafts, missiles, and spacecrafts.	*link*
Database Designer	Specify the database's logical structure, processes, and information flows.	*link*
Data Scientist	Find and interpret data, ensure consistency of large datasets, build mathematical models using data, and create visualisations to aid in understanding data.	*link*

[5] On 28th January 2022, the EU Commission has published the new version of ESCO. The two-year process review led to the integration of new job profiles and competences, some revisions in terminology for transversal skills, new labels for Green, DigComp, and Research skills and several quality improvements.
The Commission thanked the ASSETS+ Consortium together with all the organisations who contributed to the update of ESCO and the release of ESCO 1.1.
https://ec.europa.eu/esco/portal/news/e9e0f876-3f04-4a23-8524-2a5391a586f9

Top job profiles in Defence		
Job title	**Job description**	**Link to ESCO taxonomy**
Security Architect	Advise and implement solutions to control access to data and programs and ensure the protection of the organization's mission and business processes.	*link*

Table 1 - Top job profiles: descriptions and link to ESCO.

3.1 Capabilities Area: Autonomous systems

Description and overview

Aerospace engineering refers to the study and the application of the science of designing, building, operating aircrafts, and the science of flight. It addresses aircrafts and helicopter, as well as newest military aviation includes Autonomous Systems, e.g., Unmanned Aerial Vehicles (UAVs), also known as drones, and satellites and technologies for space exploration.

In the last decade, autonomous systems and drones has opened new potential scenarios in Aerospace engineering, giving to operators the support of new advances technologies. The duplication of the environment in the digital environment is enhanced by digital twin and cyber physical systems. Therefore, the goal of aerospace engineering is enlarging, also encompassing the development of productive relationships and interfaces between humans and machines, to ensure a proper and efficiency use of the emerging technologies.

This calls for well-skilled workers, capable not only to build autonomous systems, create and use virtual model and digital tools in line with operational and design issues, but also to guide and supervise those intelligent systems in compliance with legal and ethical requirements.

Capability Area: **Autonomous Systems**	
Key figures	• **Job profile**: Aerospace Engineer • **Skills**: Apply Reverse Engineering; Create A Product's Virtual Model; Using Digital Tools For Processing Sound And Images; Human-robot Collaboration; Robot Programming; Systems Engineering including safety and security • **Technologies**: Helicopter; Drones; Digital Twins; Autonomous Systems; Cyber Physical Systems; Intelligent Systems; Soft Robotics; Navigation and Vehicle Control System
Key facts	• Even if autonomous during the operations, these systems will require **increased effort** in their **design** and their **maintenance**. • The **psycological impacts** (decoupling, concentration issues) of using autonomous systems for defence must be managed. • **Safety and security** aspects will be critical for achieving **trustworthy** certifiable systems • Monitor and contribute to development of **Technical Standards** and **guidelines** for use of AI in Defense and other high **reliability** and/or critical systems system (e.g., SAE G-34, Artificial Intelligence in Aviation, and SAE G-32 Cyber Physical Systems Security Committee)
Keyword	**Integration** Autonomous systems are related with the development in AI, expecially in deep neural networks and black box systems in general. Reaching a greater explainability in the AI generated models is criticall for the development of these systems.

Figure 2 - Overview of the capability area Autonomous Systems.

Job and skills future trends

Aviation is a thriving sector and leading sector for innovation and will play an important role in the future decades in the defence sector.

Aerospace engineers maily deal with design and develop aircrafts and aerospace equipment. They program and coordinate plans for the various stage of aircraft lifecycle. Their expertise and knowledge are fundamental in air warfare research projects, development of new equipment and vehicles, improvement in engine performance and efficiency, as well as maintanance and repair operations.

The development of new flying vehicles equipped with intelligent systems and the emergence of autonomous means of transportation are changing the career path of this professional,

The key areas of science and technologies of termodynamics and fludodynamics, as well as engineering and manufacturing, will be integrated with artificial intelligence and robotics, to properly integrate intelligent and autonomous systems in the aircraft of the future since the first stage of the design process. In addition, the increasing importance of data will affect also the aerospace domain. In fact, the use of IoT sensors and devices (e.g., to study how to increase the efficiency of engines) determine the generation and acquisition of a great amount of data.

Therefore, data handling toghether with robotics and principles of artificial intelligence will be fundamantal capabilities to develop for the future generation of aerospace engineers. A key priority is to promote a stronger co-operation between the industry, universities, and VET providers to improve education and training programns in lines with the requirements of the fourth industrial revolution.

3.2 Capabilities Area: Cybersecurity systems

Description and overview

Beside the traditional Defence areas of Land, Air, Sea and Space, nowadays Cyber is acknowledged as a key domain because of the widespread utilization of digital devices and applications. The networks are becoming more and more complex, due to the interconnected systems and devices used in daily operations. Therefore, cybersecurity plays a critical role in military command and doctrine. In fact, the goal of cybersecurity is to develop and apply protection measures and procedures for the information security.

Therefore, the importance of such tasks in Defence context is closely linked to the increasing digitalization and automation of the processes. Indeed, those enabled advances in product development, processes efficiency, data analysis, and other powerful activities leveraging on the high-density connection among different and vary devices. However, the connection itself caused also risks. In fact, the vulnerability of the system increases, and its capabilities decrease, as the weaker element of the chain may compromise the integrity of the whole system. New types of attacks and threats arise, from cybercrime to hacker attack, from ransomware to phishing, from denial of service to data leak, and so on and so further.

Consequently, new cybersecurity strategies and approaches are needed to monitor and secure the complex network. Future experts will develop and execute security procedures to secure the networks and all the embedded systems and integrated components.

Capability Area: **Cybersecurity systems**	
Key figures	• **Job profile**: Security Architect • **Skills**: Embedded Systems; Integrate System Components; Prepare and Apply Security Test Plans; Secure Network Communications; Use Reservoir Surveillance • **Technologies**: Encryption; Firewalls; Intrusion Prevention Detection Systems (IDS/IPS); Battlefield of Things, Deception Technology; 5G/6G; AI for Cybersecurity; Hardware and Software Security (incl. secure supply chain of Open Source and/or third-party software)
Key facts	• Cyber security is re-shaping the defence sector, creating new **(virtual) spaces to defend**, and thus new job profiles to **manage** these spaces. • These systems are the most challingengig pedagocilly speacking. To increase people skills in cyber secturity there exists the need to **create real-life scenario**, hard to be created considering data considentiality.
Keyword	**Integration** Cybersecurity systems, even if new, are going to be drastically changed under the pressure of high-performance computing. It is still hard to foresee how these two systems wil interact in the future and investing in soft skiils related to cyber is thus. Crucial.

Figure 3 - Overview of the capability area Cybersecurity systems.

Job and skills future trends

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 intensify awareness of cyber risks both at the top-level management of organizations and among the operators in the (battle)field (e.g., ships, crews). Indeed, in the head department, CISO, 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. Then, also the operators who are the final users of systems and devices, needs to have, at least, basic level of cybersecurity expertise to effectively handle daily tasks. Thus, it is important to gain these skills for managerial and operative positions. Moreover, the increasing complexity of the systems requires a novel and stronger approach in plans and procedures for security in the software development and deployment process.

Therefore, the Security Architect is a crucial professional in every company, especially in Defence where confidentiality and security are on the strategic agenda. This profile is responsible for maintaining the security of a system infrastructure, anticipanting and

avoiding possible unauthorized access. They need to investigate on the possible failure and weakness of the systems and develop creative and intelligent solutions to set up proper countermeasures. They develop plans and procedures for security and vulnerability tests.

In addtion, the increasing amount and heterogenity of data shared in the network (indicated in the defence area as C4ISTAR big data), the faster generation of mobile connectivity (5G/6G) and the evolution in computer engineering (Quantum Computing), call for new alternative methods and approaches to the current cryptography. To face this challenge, new cutting-edge approaches leveraging on AI are being developed within cybersecurity frameworks. So, a complet skills set includes the novel technical competences, the administrative knowledge, strategic thinking, and creativity.

3.3 Capabilities Area: Intelligent Information Systems

Description and overview

Information Systems (IS) indicates the architecture for collecting, processing, storing, and distributing information. The IS includes a technical element, i.e., hardware and software, a social component, related to the people who use the systems, and an organizational perspective, related to the plans and the procedures describing tasks and roles of the users and rules for human-machine-interaction. All these elements revolve around the data, i.e., the records processed by the systems to gather useful information.

The huge technological advances in the last decades and the digital transformation enabled the possibility to exchange a great amount of data nearly in real-time. This phenomenon actually is revolutionizing the approach to data and knowledge of workers and in general of people. In addition, the development of new algorithms and procedures to process and analyze the so-called Big Data, with reference to Data Science tools and methods and so Artificial Intelligence, Machine Learning and Deep Learning, have completely transformed and enhanced our capacity to interpret the world and the events.

In the context of Defence, digital transformation has enabled a new approach, the so-called Network Centric Warfare, with the possibility to permanent exchange information at a time never experienced before between all the entities (human resources and autonomous systems) involved in a mission. Moreover, these developments increased the pace of the decision-making cycle. The data collected from various sources and shared in the network to let each operator gathering all relevant information outline a strong dichotomy between the physical and digital elements, confirming that data and information supremacy are becoming the key to achieve the goals of a mission.

Therefore, Defence players, both as national authorities and commercial organization, play a critical role in developing and strengthening skills and technical capabilities to properly exploit the value of the data and manage the risks of their malicious usage. The main challenges to face relate on one hand with the development of IS to support daily operation and mission and enhance planning and decision making, and on the other hand with the training of current and future workers who are in charge of understanding how to deal with the harmonization of the variety of data in high-tech systems that leverage on different AI and ML algorithm to enable the potential knowledge behind them.

Capability Area: **Intelligent Information Systems**	
Key figures	• **Job profile**: Data Scientist • **Skills**: Analyse Big Data; Computer Programming; Identify Data Supporting Strategies; Real-time Computing; Scientific Research Methodology • **Technologies**: Voice Recognition; Natural Language Processing; Computer Vision; Deep Learning; Adversarial Machine Learning; Explainable AI; C4ISTAR Big Data
Key facts	• State of the art AI technologies are **open-source**. This is a game changer process for the defence sector, which is istorically based on **propietary and secret** technologies. The sector need upskillinig in this direction. • Every AI technology is in fact considerable a **dual use** technology. This is opening the **boundaries** of the defence sector, and AI professionalls can easilly spend their skills in and out the sector.
Keyword	**Integration** AI systems are potential trheats for cyber security and as a conseguence valuable defence systems. Having the right AI competences in a company means been abelt o properly defend information.

Figure 4 - Overview of the capability area Intelligent Information Systems.

Job and skills future trends

Data Scientist are a critical profile in defence companies and institutions. They leverage of Artificial Intelligence and Machine Learning to combine and exploit big data in mathematical models and simulations to identify possible pattern of meaning and gather valuable knowledge from raw data. In the defence domain, they deal not only with gathering various type of data from sensors and drones, but also with timely analysing them discovering the usable content to trasmit actionable intelligence to the operators in daily tasks and missions. Therefore, they need to develop an interdisciplinary skillset consisting of software engineering, DevOps engineering, data science and AI and ML techniques to improve the performance and the efficiency of the models because only the mix of skills let to reach the defined goals.

An important implication of the increasing use of AI and ML algorithms is the really understanding of the models themselves to properly validate the achieved resutls. So, data scientist needs also of strong mathematical theoretical background since it is only the way to develop a model in line with the expectations and be able to develop Data and AI trustworthiness certification procedure. This is particularly important in the context of cyberwarfare. Advanced troops build decision on data as analysed by AI and

ML models, however, there are a risk to consider: we can influence other machine learning algorithm, by manipulating data, to modify/influence the response of the model. And so, the systems should be stressed not only for the training but also for the testing and the validation of data to ensure the robustness of the results. In addition, data scientist should ensure the ethical supervison of technology, as AI and machine learning are going to produce scenario, they need to take into consideration the ethical implication and be able to critically analyse the results provided by AI in a shifted concept of truth. Therefore, data scientist should be able to understand and manage the potential and threats of AI.

> *«Every time you a change in the way you receive your data or you take your decision, you change the concept of truth. At the beginning we had "the truth is what we see" then we had "the truth is what the data tell us", in the near future we will have "the truth is what the AI systems tell us about the processed data". So, is necessary to understand the results received from an analysis completely done by an automatic system!»*

Moreover, data scientist working in the Defence area should be aware of the domain rather than on the technical details. Automate/support decision making process with AI and ML need to be specific for the requirements of the domain (and so the characteristic of daily operations and missions in Defence are) rather than technological specific peculiarities, to fully understand what the software is supposed to do and not only how it will do it.

Finally, this professional profile requires also transversal skills to communicate efficiently and deal with custormers. Indeed, in the near future, a stronger collaboration with end-customers and representative data recording will be necessary to properly model the algorithms recorded and collected from the operation environment. And it will be fundamental especially in the military domain, hoping towards a strong collaboration between industry, military, government and so collaboration between defence (companies) and military (nations).

3.4 Capabilities Area: High performance computing systems

Description and overview

Data are crucial in the defence and military operations, as we discussed in the previous sections. Moreover, the algorithm and the techniques used to gather and share the data among all the operators and the command centers requires a higher computational power. Indeed, if on one hand we have a huge amount of data that can be acquired in various way, on the other hand engineers are facing trouble in manage the data collected in the dedicated systems. Database Management Systems (DBMS) are the interface between the data in their logic representation (for the machine) and data in their physics representation (for the users). The main functions of a DBMS are allowing access to data through a conceptual (for the machine) and physical (for the user) scheme, data sharing and integration, data access control and ensuring data security and integrity.

Traditional computing capabilities, such as hard drives or website servers, can't no more process the quantity and the complexity of the information at a reasonable speed. New hardware and software infrastructure, such as distributed systems, can have much more computing capacity. In addition, it is necessary to have architecture able to operate with limited bandwidth and latency. Since Defence will be more and more data-driven, it is crucial to enhance the current capabilities. Indeed, the power of data is strictly dependent by the power of equipment and systems where data are stored.

Capability Area: **High performance computing systems**	
Key figures	• **Job profile**: Database Designer • **Skills**: Design User Interface; Develop Software Prototype; Distributed Computing; Embedded real-time systems; Integration Of 5G/6G Services with Cloud Services; Coordinate Technical Standards For Global Interoperability; Computing system architecture; Open Source Management • **Technologies**: Big Data; Edge Computing; High Performance Computing; Deep Neural Network (DNN) processor; AI accelerator; Quantum Computing; Fog Computing; Federated Learning; S/W Defined Infrastructure incl. Network; Containers, Virtualization and automation
Key facts	• Bringing the computation to the edge require new **AI design skills** beyond embedded software skills of today to manage efficient systems. Now most of AI engineer are used to think at quasi-infinte computantional power. • **Safety and security** aspects of the computing infrastructure will be **critical** for achieving **high performance** and **energy efficient trustworthy** certifiable systems, comprehensive combination of hardware and software knowledge will be required. • **Quantum computing** may have a huge impact on AI. What is doable now only by big clusters of serves (systems such as GPT-3) can be tomorrow done by a smartphone or any other device on the field. There is the need for skilled designers, able to **imagine the systems of the future**, and the potential impact of these systems in the sector.
Keyword	**Integration** High performance computers will impact all the ther fields. AI and robots systems will be reshaped by the new computational systems.

Figure 5 - Overview of the capability area High performance computing systems.

Job and skills future trends

Database Designer design and develop the logic and the physical representation of the data in a computer system. In the context of defence, they plan and organize the information flow, from acquisition, to collection, processing, and storage, for the Command-and-Control Information Systems (C2IS), i.e., the Decision Support Systems (DSS) for Defence companies and institutions. These systems exploit the amount and the variety of data collected during daily missions and operations, to ensure a timely information sharing and increase situational awareness. These applications require a strong database architecture to effectively exploit the potential of the data.

This professional profile, therefore, plays a key role in the development of the future generation of battlefielf management systems. They oversee the definition of the requirement of the future systems. Indeed, the application of AI in a system context call for a new design paradigm for several reasons.

Today we are focused on specific algorithms and specific tasks, but in the future combination of AI methods will co-exist also with other systems (e.g., decision tree and machine learning algorithm). So, the new architecture should be integrated. And the next generation of database designer should develop a systems thinking in the design process to see the purposes and the connection with the other applications.

At the moment we have CPUs and GPUs, but in the future, is likelly that novel hardware solutions will emerge to support the AI software even more.As a consequence, it is hard to know which will be the skills related to professionals such as Hardware Engineers or Database Engineers. What is worth to do for these professionals, is for sure to invest in a stronger comprhensions of the requirements that are typical of the defence sector, to lead the design of future data systems towards beeing compliant with the strict rules typical of defence.

Now the emphasis is on the AI algorithms and their results, but we will need to pay much more attention on the data used to train and test the models. So, the development of the new architecture should consider how to store, handle, and manage in a proper way data to ensure their validity. In the future we need certificated hardware and certificated data. Therefore, a deep knowledge in database management, backup and recovery procedures as well as data quality will be crucial for this professional profile.

The amount of data available will allow to tailor solutions to the specific requirement of the customers, however it is crucial to analyze and review the logic presented by AI/ML models. So, it is necessary to have the technical know-how about the model, an engineering background about the infrastructure where the model run, and the knowledge about the context where the model is applied to understand the implication. Consequently, database designer should be able to understand the impact of decision on overall database performance and related application interfaces and context.

4. Measurement of intangible assets of the capability areas within the technological domains

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. The work is divided in three macro technological areas, each one analyzed 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 of Madrid and Seville University.

The data-driven analysis and the brainstorming sessions with industrial experts lead to the identification of four capability areas, to focus not only on the technical assets (i.e., the technologies) but also on the intangible ones (i.e., the skills and the job profiles). Those areas, previously described in this document, are the following:

- Autonomous systems
- Cybersecurity systems
- Intelligent information systems
- High performance computing systems

For what concerns the **intangible capabilities**, an analysis of the skills and occupations addressing technologies included in each capability area has been performed leveraging on the European repositories, namely European Classification of Skills, Competences and Occupations (ESCO - https://esco.ec.europa.eu/en) for skills and occupations (ESCO) and Skills Panorama (https://www.cedefop.europa.eu/en/tools/skills-intelligence) for skills foresight. The scope of this analysis is twofold. On one hand, it allows to detect new relevant concepts besides the ones previously described. On the other hand, it leads to quantify the relevance of occupations on labor market. All the new concepts collected data are included in the "R1.3 - ANNEX 3 - Database - Tech in ESCO v1-1", here the most important statistics is reported.

Table 2 reports the 36 **skills** of the new version of ESCO (v1.1) addressing technologies of the ASSETs+ roadmap. In particular, the capability areas are reported on the first column. The skills are reported in the second column: the concept addressing knowledges are reported in italics, and the ones addressing skills/competences are reported in plain text (based on the Skill Type in ESCO v1.1). Then all the technologies included in the roadmap and mentioned by a given skill are listed with their synonyms[6] in the last two columns.

Table 3 reports the 87 **occupations** of the new version of ESCO (v1.1) addressing technologies of ASSETs+ roadmap. In particular, the capability areas are reported on

[6] The synonyms refer to terms currently used to address the technologies included in the roadmap. They are listed in the report R1.1 in the Appendix 4. "Queries for Patent Retrieval in Technologies Roadmapping". The terms included in the column synonym are only the ones mentioned in ESCO repository.

the first column. The jobs are reported in the second column, then all the technologies included in the roadmap and associated to a given occupation by the related skills (previously detected) are listed with their synonyms in the last two columns.

Capability Area	New Skill ESCO v1.1 knowledge are reported in italics, and skill/competence are reported in plain text (based on the Skill Type in ESCO v1.1)	List of Technologies in ASSETs+ Roadmap	Synonyms of Technologies in ASSETs+ Roadmap
Autonomous Systems	*Human-Robot Collaboration*	Autonomous Systems	Robot
	Set Up Automotive Robot		
	Assemble Robots		
	Embedded Systems	Cyber Physical Systems	Embedded Systems; Smart Grid; Industrial Control Systems
	Perform Smart Grid Feasibility Study		
	Control Systems		
	Design Smart Grids		
	Upgrade Firmware		
	Unmanned Air Systems	Drones	Unmanned Aircraft System; Unmanned-Aircraft Vehicle System; Drone; Remotely Piloted Aerial Vehicle; Remotely Piloted Aircraft System
	Operate Drones in Civil Engineering		
	Undertake Procedures to Meet Helicopter Flight Requirements	Helicopter	Helicopter
	Aircraft Mechanics		
	Undertake Procedures to Meet UAV Flight Requirements		
	Perform Aircraft Maintenance		
	Guidance, Navigation and Control	Navigation Control System	Guidance, Navigation and Control
Cybersecurity systems	*ICT Security Legislation*	Firewalls; Intrusion Detection System; Encryption Risk Assessment & Management Cyber resilience Certification	Firewalls; Network Security System;
			Encryption
	Military Code	Encryption Cyber resilience	Encryption
	Carry Out Research on Ground Systems		

Capability Area	**New Skill ESCO v1.1** knowledge are reported in italics, and skill/competence are reported in plain text (based on the Skill Type in ESCO v1.1)	**List of Technologies in ASSETs+ Roadmap**	**Synonyms of Technologies in ASSETs+ Roadmap**
	Cyber Attack Counter-Measures	Authorization & Access control	
	Manage Cloud Data and Storage		
	Manage Keys for Data Protection		
	Implement A Firewall	Firewalls	Firewalls; Network Security System
	Teach Computer Science	Hardware And Software Security	Software Security
	Manage Alarm System	Intrusion Prevention Detection Systems	Intrusion Detection System
High performance computing systems	*Artificial Neural Networks*	Deep Neural Network (Dnn) Processor; Deep Learning	Artificial Neural Networks
	Analyse Big Data	Big Data	Big Data
	Analyse Large-Scale Data in Healthcare		
	Smart City Features		
	E-Learning Software Infrastructure	S/W Defined Infrastructure Incl. Network	Software Infrastructure
Intelligent Information Systems	*Artificial Neural Networks*	Deep Neural Network (Dnn) Processor; Deep Learning	Artificial Neural Networks; Transformers
	Computer Vision	Computer Vision	Computer Vision
	Electrical Machines	Deep Learning	Artificial Neural Networks; Transformers
	Make Electrical Calculations		
	Power Engineering		
	Control Panel Components		
	Natural Language Processing	Natural Language Processing	Natural Language Processing
	Guide Learners in Using Assistive Technologies	Voice Recognition	Speech Recognition

Table 2 - Skills from ESCO v1.1 addressing technologies of each Capability Area.

Capability Area	New Occupation ESCO v1.1	List of Technologies in ASSETs+ Roadmap	Synonyms of Technologies in ASSETs+ Roadmap
Autonomous Systems	Autonomous Driving Specialist	Cyber Physical Systems; Deep Neural Network (Dnn) Processor; Deep Learning; Computer Vision	Embedded Systems; Smart Grid; Industrial Control Systems
	Drone Pilot	Navigation Control System; Helicopter; Drones	Guidance, Navigation And Control
			Helicopter
			Unmanned Aircraft System; Unmanned-Aircraft Vehicle System; Drone; Remotely Piloted Aerial Vehicle; Remotely Piloted Aircraft System
	Instrumentation Engineer	Cyber Physical Systems; Big Data	Embedded Systems; Smart Grid; Industrial Control Systems
	Power Distribution Engineer	Cyber Physical Systems; Deep Learning	Embedded Systems; Smart Grid; Industrial Control Systems
	Embedded Systems Security Engineer	Cyber Physical Systems; Encryption	Embedded Systems; Smart Grid; Industrial Control Systems
	Robotics Engineer	Autonomous Systems	Robot
	Robotics Engineering Technician		
	Embedded System Designer	Cyber Physical Systems	Embedded Systems; Smart Grid; Industrial Control Systems
	Embedded Systems Software Developer		
	Industrial Mobile Devices Software Developer		
	Electrical Engineer		
	Textile Technologist		
	Telecommunications Technician		
	Media Integration Operator		
	Telecommunications Analyst		
	Telecommunications Engineering Technician		
	Civil Engineering Technician	Drones	Unmanned Aircraft System;

	Civil Drafter		Unmanned-Aircraft Vehicle System; Drone; Remotely Piloted Aerial Vehicle; Remotely Piloted Aircraft System
	Civil Engineering Worker		
	Satellite Engineer		
	Helicopter Pilot	Helicopter	Helicopter
	Aircraft Engine Assembler		
	Aerospace Engineering Technician		
	Aircraft Engine Specialist		
	Aerospace Engineering Drafter		
	Aircraft Gas Turbine Engine Overhaul Technician		
	Aircraft Maintenance Engineer		
	Aircraft Maintenance Technician		
	Aircraft Assembly Supervisor		
	Aircraft De-Icer Installer		
	Aircraft Assembler		
	Aircraft Assembly Inspector		
	Aircraft Engine Tester		
	Avionics Inspector		
	Aircraft Engine Inspector		
	Second Officer		
Cybersecurity systems	Embedded Systems Security Engineer	Cyber Physical Systems; Encryption	Encryption
	Chief ICT Security Officer	Encryption; Firewalls	Encryption Firewalls; Network Security System
	ICT Network Administrator		
	Data Warehouse Designer		
	Data Protection Officer		
	ICT Business Analysis Manager		
	User Interface Designer		
	IT Auditor		
	Data Protection Officer		
	ICT Business Analysis Manager		

	ICT Network Architect		
	ICT Security Technician	Intrusion Prevention Detection Systems Encryption	Intrusion Detection System Encryption
	Fleet Commander	Encryption	Encryption
	Special Forces Officer		
	Army Corporal		
	Armed Forces Training and Education Officer		
	Defence Administration Officer		
	Army Captain		
	Lieutenant		
	Colonel		
	Armed Forces Officer		
	Sergeant		
	Army Major		
	Aviation Ground Systems Engineer		
	ICT Security Administrator		
	Digital Forensics Expert		
	Ethical Hacker		
	Cloud Engineer		
	ICT Network Technician	Firewalls	Firewalls; Network Security System
	ICT System Administrator		
	ICT Teacher Secondary School	Hardware And Software Security	Software Security
	Computer Science Lecturer		
	Security Alarm Investigator	Intrusion Prevention Detection Systems	Intrusion Detection System
High performance computing systems	Autonomous Driving Specialist	Cyber Physical Systems; Deep Neural Network (Dnn) Processor; Deep Learning; Computer Vision	Artificial Neural Networks
	ICT Intelligent Systems Designer	Big Data; Deep Neural Network (Dnn) Processor; Deep Learning	Big Data Artificial Neural Networks

	Instrumentation Engineer	Cyber Physical Systems; Big Data	Big Data
	Big Data Archive Librarian	Big Data	Big Data
	Predictive Maintenance Expert		
	Data Analyst		
	Health Psychologist		
	Clinical Informatics Manager		
	Mobility Services Manager		
	E-Learning Architect	S/W Defined Infrastructure Incl. Network	Software Infrastructure
	E-Learning Developer		
Intelligent Information Systems	Autonomous Driving Specialist	Cyber Physical Systems; Deep Neural Network (Dnn) Processor; Deep Learning; Computer Vision	Artificial Neural Networks; Transformers
			Computer Vision
	ICT Intelligent Systems Designer	Big Data; Deep Neural Network (Dnn) Processor; Deep Learning	Artificial Neural Networks; Transformers
	Power Distribution Engineer	Cyber Physical Systems; Deep Learning	Artificial Neural Networks; Transformers
	Electromechanical Drafter	Deep Learning	Artificial Neural Networks; Transformers
	Electromechanical Engineering Technician		
	Electromechanical Engineer		
	Electromechanical Equipment Assembler		
	Renewable Energy Engineer		
	Substation Engineer		
	Solar Energy Engineer		
	Control Panel Tester		
	Control Panel Assembler		
	Language Engineer	Natural Language Processing	Natural Language Processing
	Knowledge Engineer		
	Assistive Technologist	Voice Recognition	Speech Recognition

Table 3 - Occupations from ESCO v1.1 addressing technologies of each Capability Area.

Table 2 reports a well-balanced number of concepts: 17 knowledge and 19 skills/competences, including therefore both theoretical content and practical abilities related to the technologies in the roadmap. On the contrary, the distribution of concepts in the four capabilities area is shifted in favor of Autonomous Systems, which includes 15 skills and knowledge, followed by Cybersecurity Systems with 9 different concepts. Then the area of Intelligent Information Systems encompasses only 8 new competences and even few the one of High-Performance Computing Systems (5 competences).

The Area of **Autonomous Systems** addresses mainly technical knowledge dealing on one hand with robots and collaborative or unmanned systems, on the other hand with aircrafts design and maintenance. Then also procedures and methods referring to design are included, such as feasibility study (*Perform Smart Grid Feasibility Study*) and control requirements alignment (*Undertake Procedures to Meet UAV Flight Requirements*). Next, in this category smart grid are mentioned, which are electricity network for intelligent monitoring, control, communication with high levels of quality and security of supply and safety[7].

The Area of **Cybersecurity Systems** includes maily skills related to protection operations, such as *Implement A Firewall* or *Manage Keys For Data Protection*. One of the fundamental elements for professionals working in this field is then the knowledge of *Cyber Attack Counter-Measures*, which refers to the all the processes for preventing or mitigating the effects of cyber-attacks. Two other knowledge included in the Area of Cybersecurity suggest the procedural and legislative nature of the cybersecurity professions, who should adopt of appropriate procedure and legislation against activities affecting the integrity of critical infrastructures; those concepts are the following:

- *Military code*: "The code language used in specific intelligence or military organisations and operations, how to use and decipher them."[8]
- *ICT Security Legislation*: "The set of legislative rules that safeguards information technology, ICT networks and computer systems and legal consequences which result from their misuse. Regulated measures include firewalls, intrusion detection, anti-virus software and encryption."[9]

The Area of **Intelligent Information Systems** includes the various branches of knowledge of Artificial Intelligence, and so systems for image processing, text processing, and audio processing. Beside the algorithm, the design of the infrastructure is gaining focus in this area, with knowledge such as *Electrical Machines* and *Power Engineering*. Then, the usability of those systems inevitably involves a proper design

[7] https://eur-lex.europa.eu/legal-content/EN/TXT/?uri=CELEX:52011DC0202

[8] In ESCO, it is a cross-sector concept, referring to occupations in different ISCO groups. The alternative labels available are the following: armed forces encryption, armed forces cipher, military code, military cipher, military cryptograph, and armed forces code. (Source: http://data.europa.eu/esco/skill/3a6b6485-8775-44b9-aba8-0ae06a53ce2f)

[9] In ESCO, it is a sector specific concept and relates with the law area. The alternative labels available are the following: legal aspects of computing, cyber-security regulation, network and information security legislation, ICT law, ICT security legislation. (Source: http://data.europa.eu/esco/skill/7814e88f-c133-4c3b-b27f-857afa145d42)

for User-Interface, addressed here with the knowledge of *Control Panel Components* and the skills *Guide Learners in Using Assistive Technologies*.

Finally, the Area of **High-Performance Computing Systems** concerns Artificial Neural Networks and Big Data. The concepts included in this area regard other domains of applications rather properly Defence, such as Healthcare, Smart Cities and E-Learning.

Table 3 lists all the professional profiles included in the new version of ESCO and addressing the technologies of the ASSETs+ roadmap.

In the Area of **Autonomous Systems**, the profiles related to aerospace (with different level of specialization and qualification, including technicians, specialists, pilots and engineers) are a more than expected result for the presence of "*Helicopter*" among the technologies. Drones are linked to a highly specialized profile, that is *Drone Pilot*, but also appear for professions in the field of construction and aerospace. Multiple profiles are linked to the "*Cyber Physical System*" technology. These range from energy to media and telecommunications to textiles, showing the pervasiveness of digital and physical working environments now in many sectors.

The Area of **Cybersecurity Systems** includes occupations related to the technical part of the protection, with reference to the technicians, designer, engineers, and architect who deal with the definition and development of algorithm, procedure, and structure for secure data and infrastructure. Among those, both *Digital forensics experts* and *Ethical hackers* analyse information, but with a different lens. The former in a forensic manner, to identify misuse responsibility and preserve digital information. The latter in an attack mode, to simulate attacks (in accordance with industry-accepted methods and protocols) on the IT system and identify any vulnerability. Then several jobs address managerial positions, namely *Chief ICT Security Officer*, *ICT Business Analysis Manager*, and *ICT Security Administrator*, who are in charge of delineating and implementing the Information System security policies and strategies. Several profiles in this category directly address the military area, with reference to the technology Encryption, fundamental to ensure that only authorized entities have access to the information in a network.

Occupations in the Areas of **Intelligent Information Systems** and **High-Performance Computing Systems** concerns specialists and engineers using Cyber Physical Systems, Neural Networks, and Big Data. Some professions in this area regard other domains of applications rather properly Defence, such as Energy, Healthcare, Smart Cities and E-Learning.

The relevance of occupations on labor market is measured with the indicator *Future Job Prospects* from Skills Panorama[10]. A glimpse the ongoing situation in the labour market

[10] *Future Job Prospect* is a comparison between future job openings and the current employment in each occupation. It is based on the forecast of future job opportunities and on the future labour market trends in Europe. The score is considered high if it is above 60, meaning that there will be high job prospects, and so more job opportunities can be opened for the given occupation compared to the ongoing situation. The score is considered low if it is below 40,

is provided in Table 4, where for each occupation the *Future Job Prospects* indicator is provided. In particular, the four occupations already included in the roadmap in Figure 1 are highlighted in bold, while the new occupations from the updated version of ESCO listed in Table 3 are reported in plain text.

Occupation	Future Job Prospect		Occupation	Future Job Prospect
Big Data Archive Librarian	100		Aircraft Engine Tester	43
Media Integration Operator	100		Avionics Inspector	43
Defence Administration Officer	74		Aircraft Engine Inspector	43
Health Psychologist	68		Second Officer	43
Data Protection Officer	68		Robotics Engineering Technician	43
Autonomous Driving Specialist	63		Electromechanical Drafter	43
Predictive Maintenance Expert	63		Electromechanical Engineering Technician	43
Instrumentation Engineer	63		ICT Intelligent Systems Designer	42
Mobility Services Manager	63		Data Analyst	42
Satellite Engineer	63		Embedded System Designer	42
Telecommunications Analyst	63		Embedded Systems Security Engineer	42
Aviation Ground Systems Engineer	63		Embedded Systems Software Developer	42
Aerospace Engineer	63		Industrial Mobile Devices Software Developer	42
Textile Technologist	63		ICT Security Administrator	42
Language Engineer	63		Digital Forensics Expert	42
Robotics Engineer	63		**ICT Security Engineer (aka Security Architect)**	42
Electrical Engineer	63		Chief ICT Security Officer	42
Power Distribution Engineer	63		Ethical Hacker	42
Electromechanical Engineer	63		ICT Network Administrator	42
Renewable Energy Engineer	63		Data Warehouse Designer	42
Substation Engineer	63		ICT Business Analysis Manager	42
Solar Energy Engineer	63		**Database Designer**	42
Clinical Informatics Manager	58		User Interface Designer	42

meaning that there will be low job prospects, and so less job opportunities for the given occupation compared to the ongoing situation. A score between 40-60 means that the number of job openings is closer but below the current employment.
(Source: https://www.cedefop.europa.eu/en/tools/skills-intelligence/future-job-prospects?country=EU27_2020&year=2020-2030#1)

Occupation	Future Job Prospect		Occupation	Future Job Prospect
Armed Forces Training And Education Officer	52		It Auditor	42
E-Learning Architect	52		ICT Network Architect	42
E-Learning Developer	52		Cloud Engineer	42
ICT Teacher Secondary School	52		Knowledge Engineer	42
Computer Science Lecturer	52		ICT System Administrator	42
Assistive Technologist	52		**Data Scientist**	42
Aircraft Engine Assembler	44		Civil Engineering Worker	39
Aircraft Assembler	44		Telecommunications Technician	29
Electromechanical Equipment Assembler	44		Security Alarm Investigator	29
Control Panel Assembler	44		Telecommunications Engineering Technician	21
Drone Pilot	43		ICT Security Technician	21
Civil Engineering Technician	43		ICT Network Technician	21
Civil Drafter	43		Aircraft Engine Specialist	12
Helicopter Pilot	43		Aircraft Gas Turbine Engine Overhaul Technician	12
Aerospace Engineering Technician	43		Aircraft Maintenance Technician	12
Aerospace Engineering Drafter	43		Aircraft De-Icer Installer	12
Aircraft Maintenance Engineer	43		Aircraft Assembly Inspector	3
Aircraft Assembly Supervisor	43		Control Panel Tester	3

Table 4 - Relevance of occupations on labour market, measured with the indicator Future Job Prospects from Skills Panorama.

Almost one quarter of the occupations (22 out of 91) register a high Future Job Prospect. A score above 60 means that more job opportunities can be opened for the given occupation compared to the ongoing situation.

The occupations in the top of the chart are *Big Data Archive Librarian* and *Media Integration Operator*. Both works with big data, the former for classification, the latter for integration. Those functions result to be fundamental in data fusion processes related to daily operations and military missions to ensure the situational awareness. Indeed, the availability of the information in the "right" moment can be essential for the success of the operation. In this sense, a continuous monitoring and update of data and metadata ensuring the compliance with standards and requirements, and, on the other hand, network operability requires synchronisation and distribution of communication signals coming from different sources. Therefore, those two profiles, apparently very distance from the Defence area, are instead very relevant. Their growth in labour market for many different industries, is a signal of a transversal labour market needs, which affect both Defence and Civil areas. Then, Defence Administration Officer takes the third place of the chart. This profile is a managerial one, dedicated to administrative

tasks in defence institutions, related both to management of Human Resources, assets management, and financial accounts.

Other jobs with growing forward-looking perspective relate with the field of Aerospace (such as *Satellite Engineer*, *Telecommunications Analyst*, *Aviation Ground Systems Engineer*, *Aerospace Engineer*). The other professions with increasing future job opportunities regard other domains of applications rather properly Defence, such as Energy (e.g., *Renewable Energy Engineer*), Healthcare (e.g., *Health Psychologist*), Smart Cities (e.g., *Mobility Services Manager*).

Some occupations worthy of mention are the ones registering a score of 52, which are in between the category of growing jobs and stationary jobs. Those refer professionals in the Education field. The *Armed Forces Training and Education Officer* properly concern the Defence industry. Then the other (i.e., *E-Learning Architect*, *E-Learning Developer*, *ICT Teacher Secondary School*, *Computer Science Lecturer*, and *Assistive Technologist*) regards the use of technologies in learning environment, both for the design and the implementation of digital learning activities.

Finally, a small part of the occupations is positioned in the lower part of the chart (12 out of 91) with a score lower than 40, meaning that there will be less job opportunities for the given occupation compared to the current situation. Those profiles are mainly operators and technician.

Besides the profiles reported in Table 4, some occupations mentioning the technologies of the roadmap do not have the Future Job Prospect indicator. Those are the ones of the ISCO group 0, which is Armed forces occupations. Indeed, this group is not monitored in Skills Panorama, therefore information about possible career development is not provided. Those profiles mainly relate with the technology *Encryption* and the skill *Military Code* and are following reported with the link to the description provided by ESCO.

Occupation	Description	Link to ESCO
Fleet Commander	Fleet commanders ensure that naval vessels are ready for inclusion in operations, and are maintained in compliance with rules and regulations. They also supervise naval personnel and are responsible for the operations of the naval service.	http://data.europa.eu/esco/occupation/0b1d8dcb-d941-4d79-99bf-fc10c1806c43
Special Forces Officer	Special forces officers operate in specialised missions such as counter terrorism missions. They perform combat and intelligence missions in order to impede with enemy equipment and installations, and to gather information on enemy strategy and movement.	http://data.europa.eu/esco/occupation/1de91afd-9da2-47ab-a7e7-19bf931709a4
Army Corporal	Army corporals supervise sections of soldiers and perform instruction duties. They also command equipment such as heavy machinery and weaponry.	http://data.europa.eu/esco/occupation/4a3f40a8-0587-494c-b8d3-7098b8c5992f

Occupation	Description	Link to ESCO
Army Captain	Army captains aid in the supervision of large units of soldiers, as well as perform planning and strategic duties in tactical operations. They also ensure equipment maintenance and provide support in logistic matters as well as support during operations.	http://data.europa.eu/esco/occupation/9bf4c8ea-e814-4772-ae31-0f29672dc497
Lieutenant	Lieutenants command troops of platoons of soldiers and lead them in training and discipline exercises. They also perform administrative duties, and function as advisers.	http://data.europa.eu/esco/occupation/b223f402-0318-4e27-8691-df6e7f7295d2
Colonel	Colonels serve in the staff of a military commander, and function as primary advisers in operational and strategic decision-making to senior officers.	http://data.europa.eu/esco/occupation/b864c9a3-ef6e-46a0-a40c-66188f74dfa7
Armed Forces Officer	Armed forces officers supervise operations and manoeuvres, assign duties, and command subordinate staff. They ensure efficient communication within and between units and perform training duties. They also operate equipment and supervise equipment maintenance.	http://data.europa.eu/esco/occupation/c6a26e11-bdf1-47a1-849d-fdcf819d458d
Sergeant	Sergeants command squads as a second in command. They allocate tasks and duties, supervise equipment, and ensure proper training of staff. They also advise commanding officers and perform support duties.	http://data.europa.eu/esco/occupation/cb3b2662-774a-4e6f-841e-f120244d7031
Army Major	Army majors command large units of officers and soldiers, supervise their training, and oversee their wellfare. They also supervise their administration, and equipment management.	http://data.europa.eu/esco/occupation/e4c915ff-6c9c-4fa9-a8fb-09d0c67e30d4

Table 5 - Armed forces occupations from ESCO v1.1 addressing technologies of each Capability Area.

5. Conclusion

The goal of the ASSETs+ project is developing education and training courses to reskill and upskill the current and future workforce in the Defence sector with reference to the emerging technologies in the domain of Robotics, Artificial Intelligence, Autonomous Systems, C4ISTAR and Cybersecurity. Therefore, a deep understanding on the trend and possible future evolution in these domains is fundamental to properly find and define the lines of actions.

The activities carried out by the ASSETs+ within the WP1 *Technology and skills analysis* aim at understanding, formalizing, and anticipating defence skills needs and technological trends. The first part of the analysis was dedicated to the delineation of the technological domains and the skills needs, leveraging on a data-driven approach based on the analysis of technical and scientific documentations (patents, scientific publications, domain-related articles, industrial reports, and so on) with Natural Language Processing techniques. We identified, measured, and classified 97 technologies, 59 defence-related applications, 172 skills, and 181 job profiles (fully described in the Annex 1). The second part of the analysis was dedicated to the experts' involvement to look at the ASSETs+ technologies in a holistic and future-oriented way. We realized several brainstorming sessions and collected more than 150 ideas exploring 3 different perspectives, i.e., *technologies and applications*, *job activities*, *education and training* (fully described in the Annex 2).

Contrasting and comparing the information gathered we developed the roadmap described in this document, which provides a wide pICTure of the Defence landscape in the above-mentioned domains. The roadmap includes the most relevant *job profiles*, the most relevant *skills* for each job profiles and the most relevant *technologies*. The technologies are positioned around the job profiles, considering the importance of a technology for a given job, and along the radial dimension, considering the level of maturity of a technology. In this way, the technologies, the skills, and the job profiles are distributed in four main areas, namely *Autonomous systems*, *Cybersecurity systems*, *Intelligent information systems* and *High-performance computing systems*, i.e., the ones that are shaping the transformation of the Defence sector. In this document a detailed description on the future trend and perspective in HR is discussed, with reference to 4 main job profiles and their skills to properly exploit the identified emerging technologies.

To summarise the final implication for the Defence sector at the European level, we rely on the framework V.U.C.A. (acronym of Volatility, Uncertainty, Complexity & Ambiguity), since it supports a proactive approach in facing the challenges of a fast-evolving operative context.

- **V**OLATILITY à Defence industry must be prepared to properly respond to the current volatile situation: the international tensions between the various nations, both from a political and economic point of view, inevitably impact on the sector, given its strong strategic connotation, increasing the instability of the already

highly competitive market. Institutions need to manage at a short notice for any contingency, and companies need to provide a swift and befitting solutions to face the posed challenges. A new agenda for strengthen managerial skills in Defence is gaining momentum: an agile and adaptive management approach is necessary to develop flexible solutions to consistently meet the need of the sector; a committed and collaborative management approach is the key capability to promote the synergic integration along the supply chain across different industries (both Defence and Civil related) and the development of shared operative model among manufacturers, customers, and suppliers.

- **U**NCERTAINTY à Nowadays technological development is not only faster but also more complex than in the past. Technological complexity is a concept linked to the need of different competencies to exploit the new technological knowledge, to the combination of different technologies in one product, and to the number of actors involved in R&D process. This high-speed and tangled technological development is radically changing the traditional innovation paradigm, towards a shift civil-defence and/or a synchronous and synergic R&D process. New patterns of interactions are necessary to create an environment for innovation, research and development, leveraging on the proximity conditions among firms, universities, and research bodies to build a strong connection among them and create an innovation ecosystem with the focus on National security and to gain and maintain EU sovreignity. Therefore, the ability to manage changes and the unsteady direction of innovation mechanisms, together with the ability to collaborate will be key competences for emerging challenges.
- **C**OMPLEXITY à Digital transformation has enabled a new approach in warfare, the Network Centric Warfare, with the possibility to permanent exchange information at a time never experienced before between all the entities (human resources and autonomous systems) involved in a mission. These developments on one hand increased the pace of the decision-making cycle, but on the other hand present new challenges for the current and future workers. The dichotomy between what is material (activities) and what is immaterial (data and information) and the acquisition of a great and vary amount of information with several sensors requires well-suited knowledge and skills to properly manage big data in various formats and harmonize them (data fusion), in order to extract and communicate the informative content to support the processes of real-time information sharing and fast-paced decision-making. In addition, the security procedures and the cybersecurity come to be fundamental to protect the network and keep its capabilities to accomplish a mission.
- **A**MBIGUITY à One of the most critical challenges in the use of Big Data and AI/ML algorithm is fighting against biases that affect the dataset and the models. Those are systematic errors deriving from wrong assumptions of the model. Therefore, the results will be influenced by these foundational errors. This is dangerous when the algorithms guide and support decision making process, and it is even more risky in particularly operative context such Defence ones. Therefore, data scientists and machine learning specialists, during the various phases of the

model's development, must be aware and apply strategies to mitigate the negative effects of the biases and develop data and AI trustworthiness certification procedure to ensure the robustness of methods and results. The considerations above imply also the importance of knowing and appling technical standards and EU regulations related to ethical supervison of technology, to ensure a legal and ethical behaviour of AI and ML models.

Given the results of these first two years of ASSETs+, and the evidence coming not only from the project, but also from other synergic activities at a European level, we can conclude that we are moving towards a defence sector that is increasingly central in Europe, and that as in the past, can lead innovation (also educational) and be a model for other sectors. The emerging technologies and their effects on human resources analysed in these reports are no longer just buzzwords, instead the pervasiveness of the applications involging autonomous intelligent systems, the urgent need of secure the cyberspace, and the demand of increasing comuting capacity recorded in recent years demonstrate how those trends are and will shape the future, not only in Defence industry but in general in all the sectors.

Therefore, it is essential to understand the facets of this complex environment, fostering the possible interrations among those cutting-edge technologies, the implication on well-suited competences and soft skills, and the good practices to deploy at the organizational level as well as on the regulatory one.

Now, we have just analyzed a part of the puzzle, but some pieces are still missing to have the complete full pICTure. Our next goal is harmonizing those valuable insights in a homogeneous knowledge base that will feed the ASSETs+ BOK.

In addition, we report the key priorities for education and training programs design, drawn from the consideration above and the valuable insights collected during the brainstorming sessions with the panel of experts from the ASSETs+ Consortium.

- The industry should be involved in education. Academic and industrial points of view are essential for the learning process. And enable peer-to-peer learning across industries to boost courses with practical problems.
- 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. The courses should be easily accessible also for practitioners to reskill and upskill competences of current workers and engineers in Defence companies and institutions.
- Increase the awareness on the Defence sector. This industry is facing troubles in get well skilled people since those are employed in digital industry.
- 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.

- It will be essential for future workers to fully understand and have the ability to use open-source and community developed components and to manage different programming languages, it is not just about learn tools and rules for programming, but also learn the differences among the available tools.
- Teach on how to distinguish good data from bad data. Nowaday students are able to understand and evaluate which are the good information and good source of information and distinguish them from opinion. The same will be with the data: future workers will need to understand which are the representative ones of a good dataset or population, and if there are trend or some is influenced by biases.
- Take inspiration from best practices. There are several training modules of cloud providers such as Azure, AWS and Google. Cloud providers already have certification programs for different roles, for instance solution architects for data scientists, for data engineers or for DevOps engineers. There are many certification programs based on many different roles and hands-on education. So, these programmes could be a great opportunity both for who starts from scratch and seniors.

At this point, if reached, will lead to more ambidexter organizations, able to explore and exploit new opportunities at the same time. This is a strong requirement to survive in a V.U.C.A. Defence world.