Deliverable R1.2
Defence Technology Roadmap

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:	**Defence Technology Roamap**
Deliverable number:	R1.2
Responsible partner:	**AAU**
Contributing partners / fellows:	**UBX, PRZ, UCIII, UNIPI, 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	December 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	March 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.3	(list all reviewers)* UCIII	Jose Maria de Fuentes	October 2022
Released by:	V.3	(Task leader)* UNIPI	Irene Spada	December 2022
Reviewed and Reselased 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 figures

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 technological 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].

[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*.

The rest of the document is structured as following: in the *Section 2* there are the description of rationale of the roadmap of technologies, skills, and job profiles and then 4 parts focus on the 4 capabilities areas (defined in the roadmap). In each of those there is a descriptive overview of the area, then the emerging technologies are defined with reference to the possible applications in the Defense sector and highlighting future trends and synergies. Finally, the overall conclusion and the key insights for the education and training programs design are reported in *Section 3*.

2. Defence Roadmap

The ASSETs+ 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.

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 ASSETs+ roadmap 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]

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

[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

[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.

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.

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 profiles* according to the identified skills.

The results of this first analysis are reported in the ANNEX 1, where the technologies and the applications 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.

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

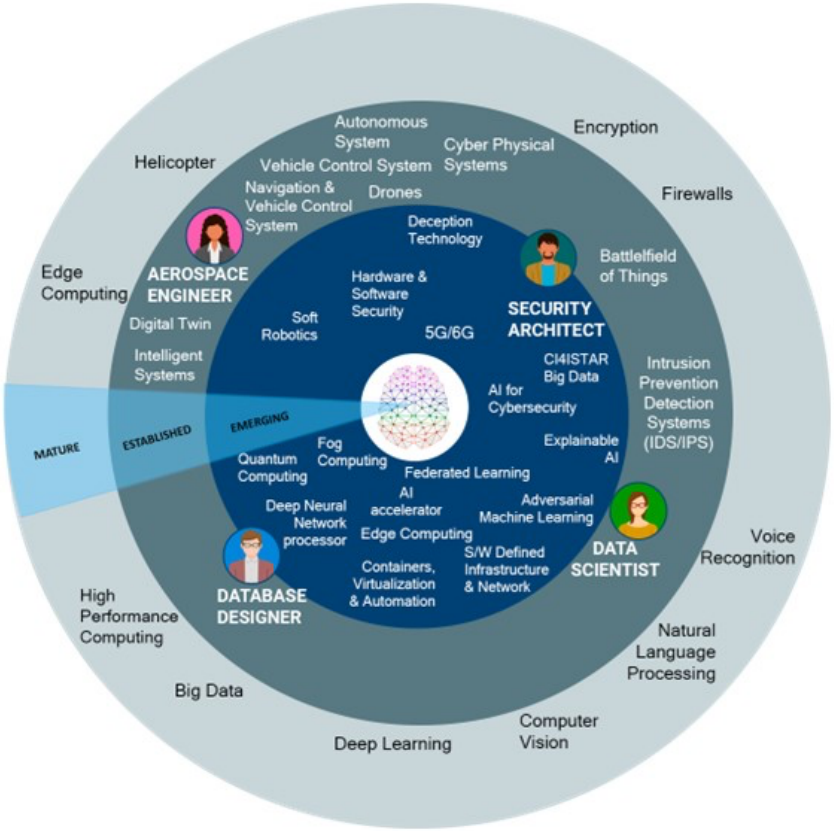
[4] This is a twin annex for the Skills Blueprint.

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

2.1 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	• The design of digital twin of physical assets requires a detailed **modelling of the information flow** in two directions (in-out and vice versa) • The **cognitive modelling** can be used to simulate or predict human behaviour or performance on tasks like the ones modelled and improve Human Machine Interaction. • The design of the physical assets should consider the integration of AI, ML, cloud computing technologies, towards **embedding AI on the edge**.
Keyword	**Integration** Human workers and increasingly high-tech components - whether hard or soft - will inevitably interact and boost daily operations and missions.

Figure 2 - Overview of the capability area Autonomous Systems.

Technologies and future trends

Helicopters are an established technology in the aerospace domain; however, they are still considered a key enabler technology in modern crisis management operations. In fact, they play an important role in daily operations and missions, due to their flexibility and modularity. Moreover, when equipped with communication radios and navigation tools (as is usually the case) they support as command posts in mission control and communication. Indeed, they allows operators to collect and share relevant and timely information on the activities to support mission execution, supervising and adjusting mission parameters using human-machine interface.

Drones, or Unmanned Aerial Vehicles (UAVs), are aircraft controlled remotely by human pilots. So, they do not allow crew to board. Moreover, they can operate with a certain level of autonomy. Those are included in the wider category of **Autonomous Systems**, that encompasses several implementations, i.e., aerial, on ground, underwater, as well as hybrid solutions. These systems enhance the several defence-related applications, such as reconnaissance, surveillance, and target tracking. Indeed, drones and similar vehicles can systematically observe space, surface or subsurface, collecting a great amount of information to properly support decision making process in planning and implementing daily operations and missions. In addition, the combination of drones and advanced technologies, such as artificial intelligence, machine learning, deep learning, and cloud computing, make the autonomous systems as **Intelligent**

Systems, able to execute complex tasks without human intervention. Therefore, the correct control and supervision on those type of technologies is fundamental to ensure the achievement of the planned goals, as well as the legal and ethical requirements.

Digital Twins are the digital representation of a physical assets, that acts as its counterpart in a digital environment, enabling the **Cyber Physical Systems** to effectively manage the complexity and the interdependencies among the various elements of the C4ISTAR infrastructure, considering both human resources and technologies that interact in daily operations and missions. Indeed, digital transformation has enabled a new approach in Defence, aka 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. Moreover, these developments increased the pace of the decision-making cycle. Therefore, having the virtual representation of physical assets enhances the collection of real time data, the integration of those digital twin in intelligent systems allows the identification of valuable insights from the amount of data to mirror the real context in a detailed digital picture. The potential applications are combat simulation, target tracking, mission monitoring and planning. And the most relevant implication is the improvement of situational awareness and strategic and tactical decision-making.

Soft Robotic is a cutting-edge technology in the field of robotics. It indicates robotics machine designed and fabricated with flexible materials, enabling movements with higher degrees of freedom than for the rigid-robots with joints. In general, robotics has been growing exponentially in the last decades, in addition this sub-field we are experiencing a faster development, such soft and smart materials, compliant mechanisms, and non-linear modeling, even soft robotics is still at the first phases of technological development. Some of the visionary but tangible implementation proposed are soldier protection and augmentation with soft exoskeletons; small warms that can rapidly and accurately explore an area to support the operators and troops in navigation tasks in harsh environments. Other possible applications are wearable monitors or fabrics with sensors that can track and check the health parameter, suggesting a possible synergy between defence and civil with emerging technologies such soft robotics. In addition, the integration of such technology with intelligent systems will play a critical role in the human-machine-interaction due to the extent of possible interplays and functions activated by this soft interface.

2.2 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 causes 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	• **Automate** cybersecurity activities: leverage on **AI applications** to execute tasks (e.g., monitoring infrastructure, incident response management, traffic analysis) and enable **smart decisions** providing validation detection engine (mix of experts knowledge and data) • **Broaden the perspective** in systems protection strategies taking into account the vulnerability of the various actors in the network, whether they are **open sources** and vertical or horizontal along the **supply chain**. • Monitor the impact of **quantum computing** on cybersecurity. It is unknown, but likely high, so it will be a **game-changer**.
Keyword	**Integration** Experts in the field will use and increase their skills and knowledge to develop a security architecture that integrates all the high-tech elements that inevitably interact and boost daily operations and missions.

Figure 3 - Overview of the capability area Cybersecurity systems.

Technologies and future trends

Encryption and **Firewall** are mature technologies for encoding information. The former is based on conversion/transformation of the original representation of a given data, and only the authorization procedure can unlock the information. The latter is based on a set of rules to monitor and control the traffic in a network with an access control list; this list defines which data can be unlocked and what action can be executed. However, nowadays information management is becoming complex. On the one hand, the shifting of the innovation paradigm towards a closer collaboration among different industrial areas produced a significant growth of the supply chain and its related network of communication. On the other hand, the development of cutting-edge technologies, like quantum computing and AI applications, makes crypto mechanisms more vulnerable. Therefore, new challenges arise to protect information within Defense Industrial Base contractors, who traditionally maintain high level security standards; it is necessary to look for different approaches/technologies, also including regulation and standardization for subcontractors, to adequately protect contract and controlled information at a level commensurate with the risk. It is fundamental also to reinforce EU's technological

sovereignty, that should be based on the resilience of all the connected services and products, especially in the Defence sector.

Intrusion Prevention Detection System (IDS/IPS) is a more recent approach in security strategy, and it is based on a combination of systems. The IDS monitor the activity in the network for detecting anomalous intrusion, the IPS monitor the elements of the network for identifying anomalies or potentially damaging component or packet in the network to prevent suspicious intrusion. They could work together in parallel, as passive, or active element, or independently. This type of approach helps in improve the capability of the systems; indeed, it increases the operations security looking both for bugs and for attack. However, there are some requirements, for example to data source's reliability and interoperability with open-source systems, for which some organization can find limiting this kind of approach. Therefore, those systems are largely used but further development are needed. **Deception Technologies** identify, examine and act against computer-software vulnerability (aka zero-day). It is a first attempt of automate security operation, indeed, it operates in real time, improving the security capability of the network. Moreover, as opposed to traditional approaches, it does not produce as many alerts as the number of executed controls, but the alerts that are the results of a subsequent reports. Therefore, unnecessary alerts are avoided, providing better support to security experts in their decision-making process.

Battlefield of Things is a breakthrough technology that mixes sensors, IoT devices and cloud and edge computing for improving the operational effectiveness of military systems. This technological concept derives from the well-known Internet-of-Things (IoT) technologies, which have been widely adopted in the civil area. The use of various type of sensors on the stream (on lower bandwidth) of wireless networks determined an increasing amount of data shared in real-time in networks (on the edge and on cloud). Therefore, it is necessary not only to harmonize them to ensure that the most information content is conveyed, but also to protect them against malicious attacks. This concept leads to the so-called *cyber electronic warfare activities*, that merges cyber and electronic warfare in the same context to support, enable, protect, and collect on capabilities operating within the electromagnetic spectrum and ensuring resilience and robustness.

The need to protect communications and so secure both classified and unclassified traffic on military communications networks, including voice, video, and data, is even more urgent with the diffusion of **5G/6G**. Indeed, the new generation of mobile connectivity allows on one side a low latency communication, therefore the time in communications reduces, on the other side a high information transfer rate, so much more devices can be simultaneously connected. This produces an exponential growth of possible attacks both on devices and applications. Moreover, with the huge information flow, the difficulty of managing alerts and reports from the network rise. To face this challenge, new cutting-edge approaches leveraging on **AI** are being developed within cybersecurity frameworks. Those solutions aim at automating several tasks and check and improve information security management.

In addition, the evolution in computer engineering, with respect to the **Quantum Computing** (further detail in the following Section 4.4), will produce new challenges for cybersecurity. Nowadays, data on the network, not only military data, or governmental institutions' ones, but also the sensitive data of individual users, are encrypted: all transactions follow encryption protocols to ensure their protection. However, the unstoppable development of quantum computers could make it possible to decrypt a large amount of data, even on the order of billions of data, in a very short time, thus producing considerable problems for national security and not

indifferent international balances. Therefore, it is crucial to develop new alternative methods and approaches to the current cryptography.

2.3 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 oversee 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**: Analyze 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	• Ensure that the AI algorithms are **explainable** and **testable:** ○ The algorithm should be described to enable the certification of the products. ○ The computational procedure should be assessed for the reliability of the results. • **Combine** multiple algorithms to solve complex problems and support decision making processes • Develop **Technical Standards for AI in defence**, dealing with model **standardization**, **ethics,** and **confidentiality** issues.
Keyword	**Integration** Data from various sources requires harmonization to be properly exploited in high-tech systems with AI and ML algorithms and to gather knowledge for informed decision and boost daily operations and missions.

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

Technologies and future trends

Computer vision in a broad perspective is a scientific field. It encompasses all the techniques and tools to process digital images or videos. The goal in collecting and analyzing this data is mimic and enhance the task of human vision. Indeed, those systems are able to arrive to a very fine grain and acquire details difficult to be seen by humans, transforming input into textual descriptions or symbols to be fast analysed by operators and elicit suitable action during daily operations and missions. Even though these systems are quite mature nowadays, their relevance within defence tasks is still high. Image processing, or more in general signal processing, in combination with Artificial Intelligence and Machine Learning, is fundamental to properly gather and manipulate data from radar, sonar, radio signals, camera, sensors, and then harmonize them in the so-called data fusion, that is the process of integrating multiple data provided by any individual data source to produce more consistent, accurate and useful information. **Voice recognition** is similarly a mature technology, but again in combination with Artificial Intelligence and Machine Learning, can represent a great advance in Defence Intelligence. The possible applications may vary from communication (e.g., transcribing oral message automatically and share in the Battlefield Management System to reduce lags in communication since no time is wasted writing message) to data processing and decision making (e.g., in patrolling, analyze all together - instead of one by one - the voices detected to match identity).

In this way the **C4ISTAR Big Data techniques**, i.e., the innovative approaches of working with data from different kind of sensors and mixing various type of information at different levels of

complexity leveraging on AI and ML, can enhance the line of command, improving the interoperability for the situational awareness, making the task force adaptable to complex scenarios, and in general the performance and the efficiency of daily operation and missions. Indeed, AI methods and approaches such as **Deep Learning**, Advanced Optimisation and Anomaly Detection and Time Series are quite relevant within the Defence sector to improve situational awareness and decision-making process. Some application of ML and DP are 3D image processing, object recognition and classification, high perceptual representation of a scenario and spectrometer (IR images). In addition, **Natural Language Processing**, a subfield of text mining, allows to extract information contained in textual documents, therefore, it concerns with automatic processing of the human language in written form. Besides a suite of tools, there is also the possibility to programs algorithms for specific tasks. The possible applications within Defence sector are many and diverse. For example, machine translation can support communication and intelligence. Document classification could be used for identifying relevant information and allowing informed decision in mission programming and planning or can be useful as tool to support specialist in understanding reports of threat attacks. NLP techniques can also analyse social context and cultural backgrounds, e.g., social media analysis, to understand and adapt operations based on the emotional, social, and cultural customs, as well as predict behaviours in disaster. A future-oriented goal (maybe not that far from being realized), in the context of Data Science techniques, is to create a system that can develop the code from requirement or from a description of the expected behaviour.

As discussed in Section 4.2, the use of these cutting-edge technologies is generating also new risks to the security of the network. Nowadays, the most powerful AI tool today is machine learning (ML), i.e., algorithm that can learn automatically through data exploration in the so-called training set and can build a model based on the pattern of interaction identified in the data. The data used to train such systems can be corrupted, and the software itself is vulnerable to cyber-attack. In this sense, the ML techniques are called **Adversarial Machine Learning**. Therefore, these areas must be addressed at scale as more AI-enabled systems are operationally deployed.

Finally, a particular mention is needed for **Explainable AI**, that means certifiable and trustworthy Artificial Intelligence algorithms. 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. It is necessary to study the behaviour of the algorithm to understand the logical structure behind the model and ensure that the AI algorithms are explainable and testable. Indeed, the description of the algorithm enables the certification of the products, and the assessment of the computational procedure can demonstrate the reliability of the results. The success is essential for to deploy AI technologies, particularly to the tactical edge, where reliable performance is required. In this regard, Defence operators in Data Science are facing far from straightforward challenges dealing with which data are used for software development (SD) processes (data access, data quality), monitor the training dataset, implement features driven by data. Another challenging operation is share training models and/or training set, but in a such complex and strategic sector as Defence, this could only happen if there is a stronger collaboration in the higher level of the EU Defence stakeholders' network.

2.4 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	• **Embed AI on edge** devices to elaborate directly the data, squeeze the model and the data on the edge to ease of data processing, avoid cybersecurity issues, ensure an easy transportation of the models, etc. • **Distributed computing** resources that provide **real-time** guarantees of resources when needed for system functionality. • **AI/ML accelerators** and System on Chip (SoC) devices including **reconfigurable** processing technology • Design space Exploration to map system **functionality** to available resources that guarantees correct computing and communication **performance** when needed. • **Quantum Computing** and **Fog Computing** are shaping the future of the computational architecture.
Keyword	**Integration** Improve the the computational capacity and balance it with the power of the elaboration tools and methods. The servitization is the key to scale and properly exploited the technical solutions with data and AI/ML algorithms, to boost daily operations and missions.

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

Technologies and future trends

This capability area is characterized by a particular opposition: the technologies to be integrate are at two different level of maturity, without any transition solution between them. Indeed, on one hand we have mature technologies (Big Data; Edge Computing and High-Performance Computing) and on the other hand we have emerging technologies (Quantum Computing, Fog Computing and Federated Learning).

The digitalization of the assets calls for a fusion between those technologies, and the integration in this area could follow two opposite paths. The first one goes from emerging to mature and consist of moving AI on the edge. The secondo follows the other direction, from mature to emerging, moving Big Data on the Cloud.

The solution of embedding AI on edge devices allows to directly elaborate the data and the algorithm on a physical infrastructure which is independent from external information sources and computing resources. In this way it is possible to elaborate data and enable intelligent decision making everywhere, independently of the working condition. Therefore, new design approaches seek to tailor the hardware architecture to the AI software solutions, leveraging on the state-of-the-art processors (mature **edge computing** technologies) to boost AI capability. The advantage of this approach lies on:

- the high efficiency, since these devices could work also in constrained condition with limited bandwidth and latency or even no connectivity,
- the ease development, since the develop and test micro-chip is a well-established process,
- the safety, because the devices are decentralized and independent, so it is hard to attack them.

However, this approach does not exclude the progression of Cloud. In fact, on the other hand, it is also possible to achieve 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.

Quantum Computing is an emerging computing based on Quantum theory, in which subatomic particles can exist in more than one state. In this sense, they do not follow the traditional binary behavior of computer systems. The use of Quantum Computing in for defence applications regards intelligence, security and mission planning and control; and needs to deal with new strategies, doctrines, scenarios, and ethics issues.

Fog Computing is a horizontal infrastructure, used for seamlessly distributing computing resources and services. It connects Cloud to the Internet of Things (IoT). It mixes edge devices (to execute a big amount of operation) and cloud services on Internet (to transmit information and communicate locally). Therefore, it extends and improves cloud, some of the improvement includes the need of less bandwidth, the decentralized infrastructure, the low delay in transmission.

Federated Learning is a Machine Learning technique in which a set of agents works collaboratively to train a model. Therefore, it is not necessary to share the training set, that potentially can include sensitive data. This approach differs from the traditional training methods, where the datasets are in a local server.

More performance at lower electrical power is essential to allow both data centre 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. A trend (GAIA-X) is that Europe is more and more striving for more sovereignty and a multi-cloud approach. So, a strong cloud capability is a key pre-requisite for the industrialisation of AI and automation solutions.

3. Measurement of technical 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 analysed by a part of the WP1 team:

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

The data-driven analysis and the brainstorming sessions with industrial experts lead to the identification of four capabilities area, 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 **technical assets**, an analysis of patents[5] in each capability area has been performed. This analysis allows to measure the relevance of the areas with respect to the technological domains in analysis. The collected data are included in the "R1.2 - ANNEX 3 - Databases of Patents Metadata of Capabilities Areas and Technological Domains", here some statistics are reported.

Figure 6 presents the *Relevance of a technological domain in each capability area*, computed using the patent metadata: the number of patents resulted by each query, on all the available time window from 1842 to 2022, can be intended as a proxy of the importance of a given technological domain in each capability area.

Then, Figure 7 reports the *Trend of publication date* for each query will be included. The time window for the trend plot includes patents from 1921 to 2021, so this trend exclude the number of patents registered in 2022.

[5] The reference database will be Espacenet (https://worldwide.espacenet.com/), a free online database of patents, developed by the European Patent Office (EPO) together with the member states of the European Patent Organization.

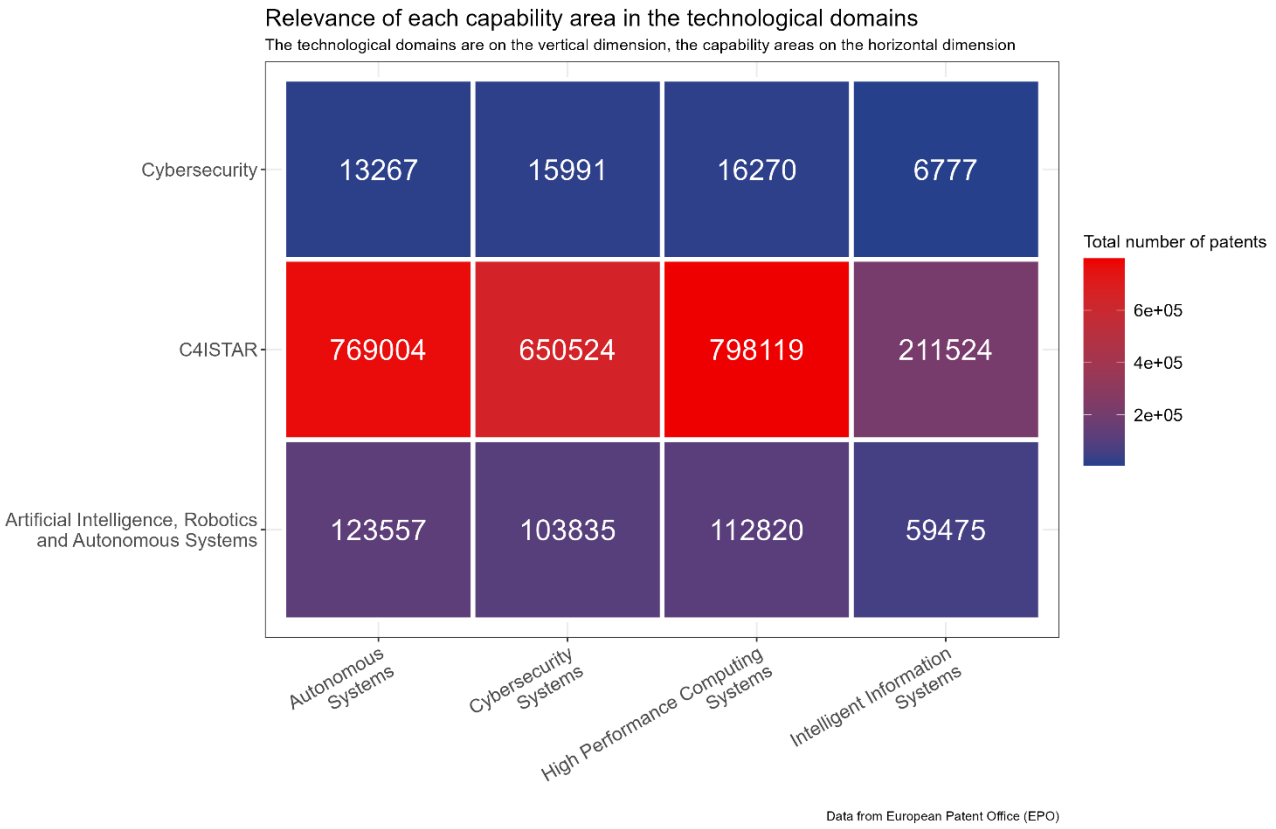


Figure 6 - Relevance of a technological domain in each capability area.

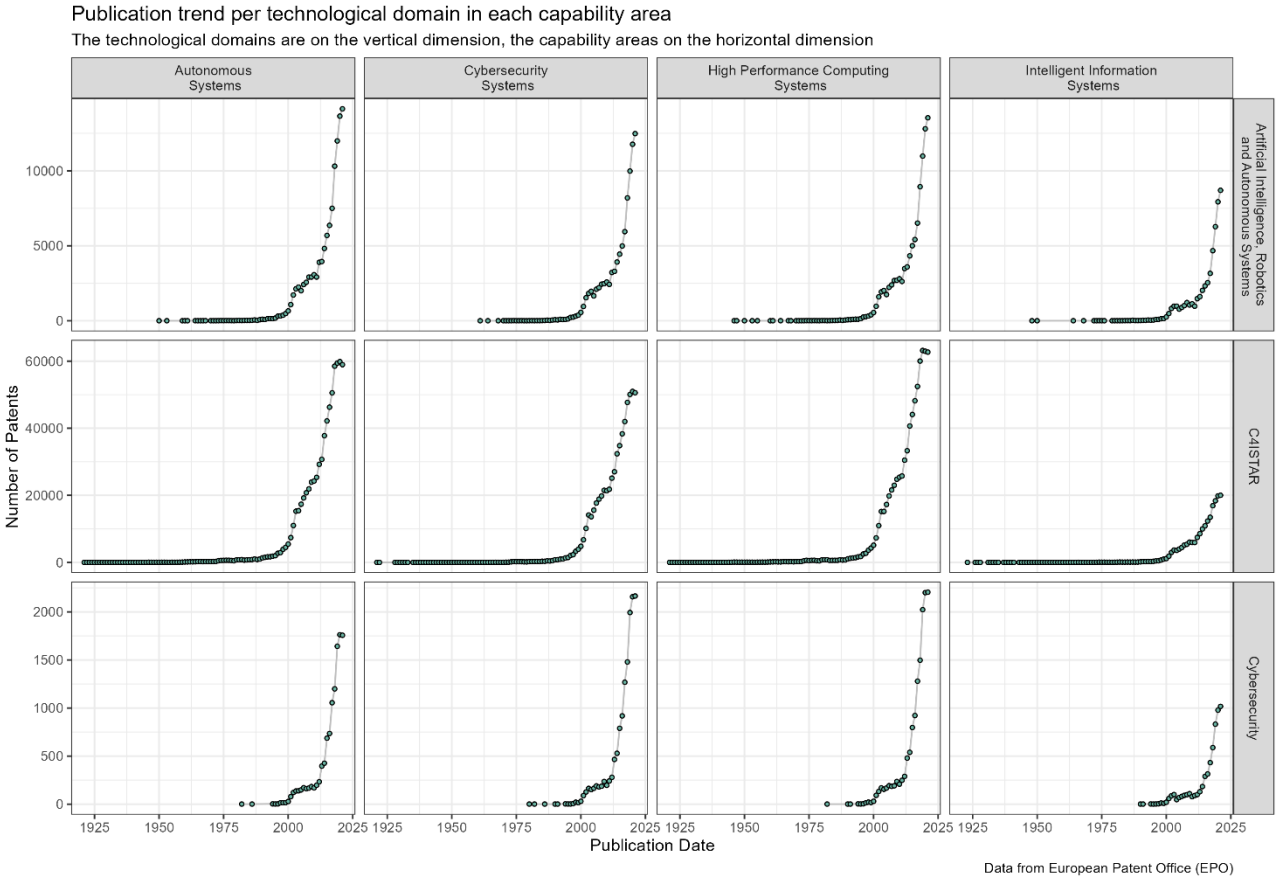


Figure 7 - Publication trend per technological domain in each capability area.

The pervasiveness of the technological domain of C4ISTAR is evident from Figure 6, as the number of patents in all the capability areas is very high. These results suggest that Command and Control operations are being improved with new technologies involving autonomous systems in close cooperation with human-forces, which leverage on novel information systems to ensure the overall supervision of all the elements involved in missions and daily operations. This leads to higher computational power and need for protection of circulating data and information. For what concerns the technological domain of Robotics, artificial intelligence (AI) and autonomous systems, the higher number of patents is registered in the capability area of Autonomous systems. A quite similar result is registered also for the technological domain of Cybersecurity and the related capability area, even thought is worth noting that cybersecurity is typically applied in other technological domains, indeed the number of patents in the capability area of High-Performance Computing is even higher due to the research and development about protection of new computational infrastructures. For both technological domains, the capability area addressing the new computational infrastructures (i.e., High performance computing systems) resulted to be very relevant, suggesting a focus on adopting novel architectures of computers and devices to process the amount of the data with complex algorithm at a reasonable speed and ensuring high level of security.

Figure 7 can be read in two directions: per row, to evaluate differences among the technological domains, and per column, to examine differences among the capability areas. The former perspective does not indicate any relevant diversity among the domains for the various capability areas, indeed the slope of the curves is similar in all the intersections, suggesting that during the analysed time window the patenting approach has been comparable for all the technologies. The latter perspective shows some differences. Indeed, the first group of patents for the C4ISTAR domains date back to the final part of the previous century: 294 patents have been published

between 1842 and 1920[6], and 1602 patents have been published between 1921 and 1950. For what concerns the technological domain of Robotics, artificial intelligence (AI) and autonomous systems, patenting had its origin around 1950, when research and studies around this discipline date back in the '50s. Finally, patents related to the technological domain of Cybersecurity have been registered since the '90s, with the increasing diffusion of the Internet. For all the technological domains, an increasing trend of patenting is evident from 2010, as the slope of all the curves tends to rise very fast until nowadays. The higher growth can be detected for the technological domain of Cybersecurity, as the distance between two subsequent points is the highest from one interval to the following.

[6] Those documents are not shown in Figure 7 as they are related to an earlier time than the time window of the graphs.

4. Conclusion

The goal of the ASSETs+ project is to develop 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 technological domains is discussed, with reference to main technologies and their defence-related applications.

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) the perfectly fits the characteristics of the modern defence sector.

1. **V**OLATILITY à Profound changes in geopolitical environment, innovation challenges in science and technologies and fast evolution in digital world are having a great impact on defence, both in sense of treats and opportunities. In fact, firms, and agencies on one hand must adapt themselves in this new context developing a new concept of war and peace missions. On the other hand, have the possibility to enrich and improve their assets and capabilities, moving towards the so called C2 Agility in the Network Centric approach. This is a process approach in mission development that considers in a harmonic perspective the structures and organizational attributes, the standards and the procedures to follow (both for operation and risk managing), the human perspective as individual and collective behaviour and the resources (including information). Also, the approach gives much more attention about activities for creating value and supporting individual and collective informative decision making.
2. **U**NCERTAINTY à the fast technological evolution makes difficult to properly delineate and address its impact in the labour market, in education and in general in the society.

In addition, a complete understanding of the technological evolution in such a complex domain like Defence (where the confidentiality of the information is critical) is challenging. Therefore, the ASSETs+ approach, leveraging both on qualitative and quantitative techniques and methods, is a feasible way to have near real time monitoring.

3. **C**OMPLEXITY → the complexity of the technologies and the blurred boundaries of the technological domains are radically changing the innovation paradigm towards a stronger cross-fertilization and contamination among defence and civil applications. Therefore, cooperating projects and initiatives will be fundamental to maintain the technological edge. Current and future workers will work together in a cross-disciplinary way to manage complexity.
4. **A**MBIGUITY à we are moving towards an industry where technologies are more and more integrated with operators in a human-machine teaming and machine intelligence. Therefore, Research and Development in platforms and environment where workers and technologies can work together must be supported also with regulations and procedures to ensure the ethical and legal behaviour of the artificial intelligent systems.

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 involving autonomous intelligent systems, the urgent need of secure the cyberspace, and the demand of increasing commuting 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 interrelations 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.

- Have professionals that know machine learning, software engineering best practices and emerging technologies that rely on this kind of science and applications in a multidisciplinary approach.
- Include in the programs a deep understanding and education about stochastic systems and statistics and a good mathematic background.
- The programs should include technical aspects beside models, such as data storage, message brokers, distributed processing, computing clusters, open-source solutions such as MLflow for model serving and registry, containerization via Docker etc.
- Move towards more transversal job profiles, that are technological experts with managerial skills. In this direction, we expect to see a growth of managerial courses for software's engineers and AI courses for manager. This can lead to an impact that goes behind product innovation, also increasing the quality of internal project managements and intra-preneurial skills.

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.