# Defence Body of Knowledge

*Authors: Ana Beatriz Lopez, Adelaide Almeida (EWF), Irene Spada, Filippo Chiarello (UNIPI)*
*Revised: Peter Nielsen (AAU)*
*Approved: UNIPI*

**Note: The document has been shared with other partners and WP leaders for gathering inputs and comments at various stages of the preparation of the document*

# Table of contents

# 1. Introduction

## 1.1 Description of the project, goals and participants

Industry 4.0, business digitalisation, artificial intelligence and KETs are increasingly taking centre stage, not as buzzwords but as pillars for innovation in all business sectors at a global level. The Defence sector is no exception.

Accordingly, all players involved in this field are experiencing evolution in both business processes and human resources: the former regarding technological advancements; the latter regarding the skills needed to exploit such technologies in the proper way.

As a response, ASSETs+ project aspires design and deliver a series of training courses that will plug the gap in existing provision and thereby reduce the skills shortages the sector faces. ASSETs+ is a part of the transnational project Sector Skills Alliances. The aim of the project can be derived from the meaning of the name: Alliance for Strategic Skills addressing Emerging Technologies in Defence.

In fact, it is set up to identify the existing and emerging skills needs for professions in the Defence sector, in order to build up training courses for the labour market.

The technological domains to address are:

- Robotics, autonomous systems, artificial intelligence;
- C4ISTAR (command, control, communications, computers, information/intelligence, surveillance, target acquisition, reconnaissance);
- Cybersecurity.

And the main topics are:

- Digital skills;
- Skills for key-enabling technologies;
- Support for European and regional innovation and smart specialization strategies.

The concept of the project is first to analyse trends in technology, then to identify the skills required to use them and so to understand what the requirement of the training programmes are.

First, identifying which competencies and skills will have an impact on the future in Defence is important, due to the Defence specificities regarding the skills shortages for the sector. Some of the extent, causes, and implications have been already outlined in previous projects, highlighting the need for a project as ASSETs+:

- Difficulties in forecasting the overall volume of the future demand for defence related skills due to uncertainty attached to future levels of public procurement, such that E&T institutions are unsure about future demand levels;

- The low volume of specialist skills required. Some skills are critically important to the sector but are needed in small volumes. This poses problems for E&T providers who require programmes to be of an economically viable size;
- Nationally segmented markets for skills where 'national eyes only' requirements make it difficult to achieve the economies of scale mentioned above, while limiting the mobility of skills between member states;
- Competition from other sectors for those with the skills the defence sector needs. This is exacerbated in some countries where working in defence is considered unattractive;
- Lack of internal training provision and mentoring programmes to develop specialist defence skills.

As it can be seen, innovation is a strategic imperative for all the players on the market for the maintenance and development of an economical sustainability and there is no exception for Defence companies: they must stay alert on the evolution of the sector to remain competitive on the market. But focusing only on technology is not enough. Companies in the Defence sector deal with sector-specific problems, as re-training the existing workforce and getting new workforce with the new skills and competencies required.

In particular, human resources need to possess or develop new and high specialized knowledge, skills and competences not only in terms ff the technologies but more relevant on how the technologies are applied within the domain. This will be possible with training programmes, that will align the education system and the labour market building up a framework for strategic cooperation, in order to support workforce adaptation at national and regional levels and to share knowledge and common practice to promote the digitalisation in the context of Industry 4.0.

To reach this goal, collaboration between different entities as labour market, education and training stakeholders and social partners is the key for the successful research and development of the defence specific skills. To be more specific the Consortium in formed by 30 partners of 8 different countries, EUPPORTUNITY (PT) and REPORTBRAIN (UK) as associate partners. In the Table 1 there is a short description of the group of participants and a list of them.

| Group | Description | Participant |
|---|---|---|
| Education system | Higher education and scientific institution and structure, public or private, divided into faculties, degree courses, departments and institutes, and in special schools, which has the task of issuing legally recognized academic and professional qualifications, as well as promoting research, the advancement of science. | University of Pisa (UNIPI) |
| | | University of Aalborg (AAU) |
| | | Université de Bordeaux (UBX) |
| | | Central Supélec |
| | | Rzeszów University of Technology (PRZ) |
| | | University of Cadiz |
| | | University of Sevilla (UNISEVILLE) |
| | | Technical University of Madrid |
| | | University Carlos III of Madrid (UCIII) |

| Group | Description | Participant |
|---|---|---|
| Vocational Education & Training Providers | Type of education institution specifically designed to prepare people to work (as a technician or in various jobs) | Consaer |
| | | Mercantec |
| | | Aerocampus Aquitaine |
| | | Royal Military Academy |
| Accreditation, certification, qualification or research foundation | The accreditation, certification, qualification organizations certify the compliance of management systems or products or personnel with specific reference standards and have the authorization to issue a certificate of conformity<br><br>The research bodies are independent public or private non-profit organizations whose statutory purpose is to carry out research, technological development and dissemination of knowledge. | Fondazione Giacomo Brodolini (FGB) |
| | | Cimea |
| | | European Federation for Welding Joining and Cutting (EWF) |
| Enterprises | Organization of goods and human capital aimed at satisfying human needs through the production, distribution or consumption of economic goods and services to customers, structured according to a certain corporate organization and administered according to a certain governance by the business management. | Leonardo |
| | | Safran |
| | | Navantia |
| | | Rolls-Royce |
| | | Hensoldt |
| | | Airbus |
| | | Saab |
| Sectoral organization | Institutions organised nationally and regionally along sectoral lines | Distretto Tecnologico Aerospaziale Della Campania Scarl (DAC) |
| | | Center for Sikkerhedsindustrien i Danmark (CENSEC) |
| | | Groupement des Industries de Construction et Activités Navales (GICAN) |
| | | Fundación Andaluza Para el Desarrollo Aeroespacial (CATEC) |
| | | Asociación de Empresarios del Sector Aeroespacial Andalucía |
| | | Asociación Madrid Plataforma Aeronáutica y del Espacio |
| | | Shipyards and Maritime Equipment Association of Europe (SEAEU) |

*Table 1 - Description of ASSETs+ participants.*

The project is divided in several work packages, as presented in the Table 2.

| N. | Work package | Short description and main output |
|---|---|---|
| 1 | Technology and skills analysis | Define the Technology Roadmap, which describe the evolution in the technology domain; extract the skill related to the technologies identified, explained in the Skill Blueprint; translate skill needs in job profiles. |
| 2 | Education and training | Design the pedagogical approach, test and validate the Education and Training Programme defined. |
| 3 | Programmes implementation | Implement a pilot of the plan, in order to review and improve it. |
| 4 | Exploitation | Exploit the plan |
| 5 | Dissemination and communication | Share the content created developing and implementing a Dissemination and Communication Action Plan |
| 6 | Quality assurance and monitoring | Develop and implement Quality Assurance and Monitoring Plan |
| 7 | Management | Overall management procedures (monitoring all the project activities and manage communication flow with EACEA and among all the partners) |
| 8 | Evaluation | Review and validation to verify they are addressing concrete industrial needs |

*Table 2 - Work package of the ASSETs+ project.*

According to the fast-technological changes and the emerging of workforce needs, it will be carried on an iterative approach (e.g. in WP1 discovering trends and steadily monitoring them, so that it could be possible to take any required action promptly). The monitoring and evaluation of the work will be based on quarterly reports (contain activities, reflections, challenges and recommendations for improvements.)

The first step will set the path of the whole project:

- it relates to all WPs for central role in developing the main strategy;
- it is closely linked to WP2 and WP3 indeed training courses will be design based on WP1 outputs;
- it interlinks with WP4 and WP5 as the results will be published and disseminated as best practices.

WP1 is divided into several tasks:

- **Strategy specification**: develop the methodologies to undertake in this WP and in general in the overall project.
- **Technology mapping**: describe the evolution in various technology domains that could have an impact on defence and how these ones could be applied, through patents and scientific papers analysis and using algorithms for automatic text analysis, in order to define Technology Roadmap.
    - The main domains and the universities to which research is assigned for each domain are:
    - Robotics, Artificial Intelligence and Autonomous Systems - AAU and PRZ;
    - C4ISTAR - UNIPI and UBX;
    - Cybersecurity - UCII and UNISEVILLE.

- **Emerging skill related to selected techs**: understand the link between technologies and skills using Technimetro® (a database of terms and relations related to Industry 4.0, its sources are technical dictionaries, newspapers, scientific articles available from academic sources and open databases on base most cited in association with keyword 4.0) and present the results in the Skill Blueprint.
- **Skills and job profiles validation**: internal validation of results.
- **Skills2ESCO**: interpret the Skill Blueprint to make it compliant for being integrated in the ESCO database (the European multilingual classification of Skills, Competences, Qualifications and Occupations). It is possible to find out existing and new jobs profiles. It will be very useful to better understand what competences and qualifications are needed to upskill the workforce in the Defence sector and so what are the requirement of the training programmes.
- **Fiches**: produce a report consisting in a list of identified relevant Defence related skills
  programmes and initiatives.

## 1.2 Description of approaches

The overall methodology adopted in the WP1 for the technologies and skill analysis balances standardization and differentiation: it ensures the coherence of results of the three technological domains and lets each team adopt an approach based on their own expertise both in technical analysis and in Defence.

As anticipate before, the domains and the universities to which research is assigned for each domain are:

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

The three teams are composed by professors, researchers and PhD students who:

- have specific skills and expertise in the fields of innovation, technologies, design educational programmes, technology foresight, data science and the extraction of knowledge from deconstructed texts of various kinds (e.g. patents, scientific articles, etc.);
- have several collaborations in Defence-related projects.

The core of the approaches is the **automatic text analysis** with the purpose to explore a heterogeneous database of resources related to the three technological domains in a quantitative way. The sources of the documents are research institutions, National or International institutions, companies, thematic websites and market surveys.

Different sources allow to:

- Reduce biases: the content of each document may be influenced by various factors (e.g. official documents by National or International institutes may be influenced by political decisions, companies may define the technology domain based on their principal competencies and products and thus may offer only one perspective). Therefore, the variety of the sources makes it possible to balance the biases of each source itself.
- Increase recall: recall is the number of relevant retrieved documents divided by the total number of relevant documents. Having a wide variety of sources increases this variable.
- Validate information: finding the same information in different documents from different sources ensures a higher quality.

Additionally, there is more than one standard of military terminology and various databases of skills available to the public domain, therefore those have been included in the sources:

- NATO Terminology database;
- U.S. Department of Defence Dictionary of Military and Associated Terms;
- Glossary in NNEC C2 Maturity Model;
- European Skills, Competences, Qualifications and Occupations (ESCO);
- National Initiative for Cybersecurity Education (NICE) Cybersecurity Workforce Framework (NIST SP-800-81).

Moreover, **Technimeter®**, a tool of developed by the University of Pisa, has been used in the analysis. It is a database of terms and relations addressing the Industry 4.0 paradigm, available in three languages (Italian, English and German). The sources for this tools are technical dictionaries, newspapers, scientific articles available from academic sources and open databases most cited in association with the 4.0 keyword. It provides hyperlinked text for a set of enabling technologies for Industry 4.0, associated to their definitions and connected between them, and a set of 4.0 skills.

Other methodological approaches used are:

- **survey to industrial partner**, to include a practical point of view since the first step of the analysis; in particular 3 surveys have been conducted during the first year of the project;
- **expert judgment**, to obtain specific information by professionals of the Defence sector, both in academic environment and in industrial one, who acquired domain knowledge thanks to the experience in the specific area.

# 2. Body of knowledge

A body of knowledge (BOK) is the ontology of concepts, terms and activities that make up a professional domain, as typically defined by the relevant learned society or professional association.

The ASSETs+ Body of Knowledge (BOK) is one of the main outputs of the project, that will map all the relevant competences needed for defence practitioners with respect to the technological scope of the project - Robotics, autonomous systems, artificial intelligence and C4ISTAR and cybersecurity, and will be a guidance document for the European Defence Sector.

The objective of ASSETS+ BOK is not only to provide a detailed analysis of the knowledge required by any person working for or on behalf of Defence Sector, but also will be the basis for the design of the courses (WP2) to apply in the ASSETS+ project.

The ASSETS+ BOK will be based on the Technology roadmap (R1.2) and on the Skill Blueprint (R1.3). Also, the Technimeter® (a tool of developed by the University of Pisa that maps skills) will be used to dynamically map job profiles and skills of the defence sector and update the BOK, assuring that the BOK will keep itself updated during and after the project. In this way the BOK will be a reference also for future courses outside of the present project.

## 2.1 Concept and Objectives

The ASSETS+ project aims at creating a strategy to up-skill defence students and professionals, including the identification and standardization of job profiles related to the technologies identified in this project. So, the concepts explored in the ASSETs+ project are the **technologies**, the defence-related **applications** and the **skills**, with the purpose to provide a framework for the design and development of the training courses.

These entities are strictly related each other's because every technological systems support some users in various activities during daily operations and missions to reach the defined goal thanks to some specific requirements of the system itself and especially thanks to the abilities of the user to correctly exploit those technological systems. Therefore, the concept analysed in the ASSETs+ project can be defined as following:

- **Skill**: characteristic of every user to perform an action, where the user is a person who uses a product, a machine, or a service;
- **Technology**: methods, systems, and devices which are the result of scientific knowledge being used for practical purposes;
- **Application**: the act of use something for a purpose.

These concepts are analysed in the R1.2 Technologies Roadmap, R1.3 Skills Blueprint, that are used as the mosaic tiles for the design of the training courses and the exploitation strategy. The huge amount of knowledge produced needs to be handle correctly to appreciate its value.

Therefore, the results are summarized in the R4.5 Body of Knowledge to provide an overview of the overall results and so an ontology of the ASSETs+ project. It constitutes a guidance for the European Defence Sector since it is a detailed breakdown of the knowledge, concepts and relationships of Defence Sector.

A reader can explore in deeper the evolution of technologies in Defence-related applications with the R1.2 Technologies Roadmap. He/she can have a complete overview on the skills landscape with the R1.3 Skills Blueprint. He/she can examine the overall perspective with the R4.5 Body of Knowledge.

These relations among concepts and documents are mapped in the Figure 1, where there the three categories of entities (i.e. technologies, applications and skills) are linked and related to the documents in which they are analysed.

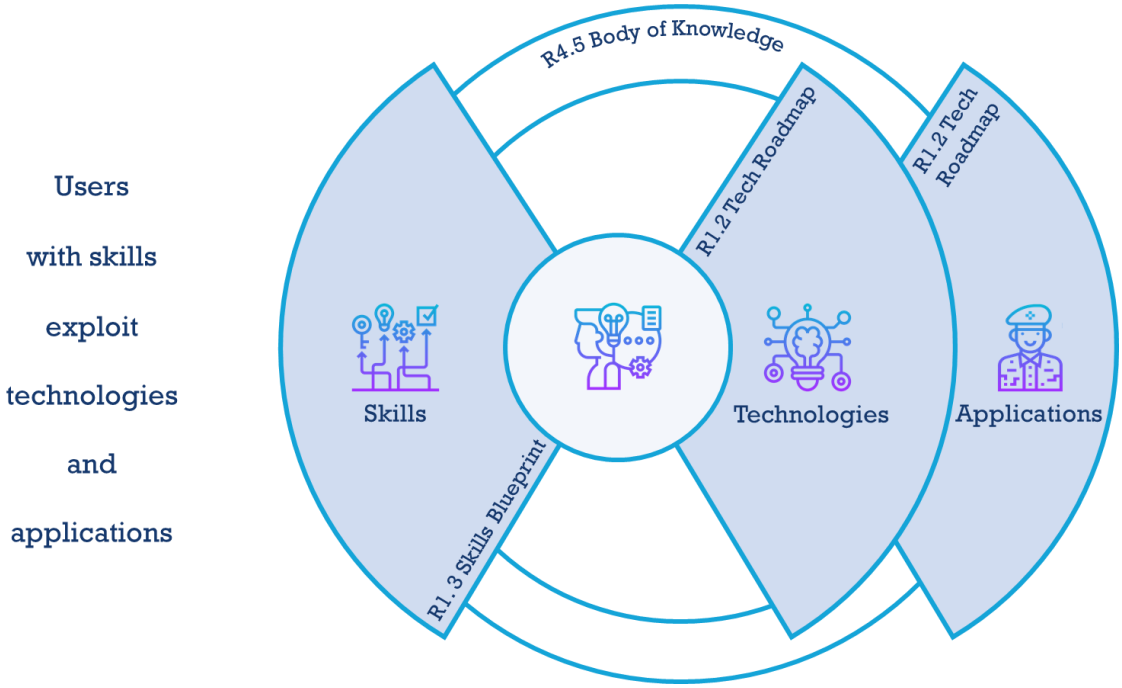


*Figure 1 - Map of relations among technologies, application and skill, whit reference to the ASSETs+ documents.*

## 2.2 Characterization of Defence Sector

The digital transformation of the last decades brings a re-shaping of many industrial sector and Defence is no exception.

This paragraph contains an exploration of this industry in terms of public military expenditure and dynamics in Defence industry in competition to provide a delineation of the context of use of the technological systems explored in the ASSETs+ project.

### 2.2.1 Analysis of public military expenditure

In recent years, European Union has begun to promote initiatives in the context of defence to provide more resources, stimulate efficiency, facilitate cooperation and support the development of new capacities. The drivers of this transformation are the defence investment breakdown, the fragmentation of defence industry and the increase of global insecurity. European Union is looking for a stronger integration between defence systems of Member States, in order to be more powerful in the global panorama, to avoid duplication of investments and to guarantee the security of European area itself.

In this sense, in 2017 the Permanent structured cooperation (PESCO) has been formed and in 2019 twenty-five EU Member States are participating. PESCO is an organization that finances and promotes project related to sectors such as training, capacity building and operational readiness in defense matters (e.g. European medical command, a maritime surveillance system, mutual assistance in cyber security, rapid response teams and a common EU intelligence school). Other project carried on are: the Global Strategy for Foreign and Security Policy and its Implementation Plan on Security and Defence, the Defence Action Plan, the Preparatory Action for Defence Research (PADR) and the European Defence Industrial Development Programme (EDIDP), the Capability Defence Planning (CDP) and the Coordinated Annual Review of Defence (CARD). An European Defence Fund (EDF) has been proposed for the post-2020 period. Finally, the EU and NATO committed to strengthening their cooperation. Implemented properly, these initiatives can make a difference and contribute to a more secure Europe[1].

It is possible to measure of the commitment of European Member States in defence sector analysing the public expenditure and investments in defence, presented in Table 3 and Figure 2, and the evolution of Gross Domestic Expenditure in Research and Development (known as GERD) from 1980 to 2018 for U.S., Europe, France and the aggregated data for OECD countries, as registered in OECD repositories[2], presented in the Figure 3.

[1] https://www.asd-europe.org/defence

[2] Data retrieved from OECD repositories searching "Main Science and Technology Indicators", using "GERD as percentage of GDP" and limiting the countries and the year range (i.e. from 1980 to 2018), available online at: https://stats.oecd.org/viewhtml.aspx?datasetcode=MSTI_PUB&lang=en. In particular, the graph of Figure 1.8 shows trends of United States and France, since they are the greater expenditure in Defence (as ranking in SIPRI Military Expenditure Database [11]), and aggregated data of the European Union 28 countries (EU-28), EU-15 and the OECD zone. The zone EU-28 includes Austria, Belgium, Bulgaria, Croatia, Cyprus, the Czech Republic, Denmark, Estonia, Finland, France, Germany, Greece, Hungary, Ireland, Italy, Latvia, Lithuania, Luxembourg, Malta, the Netherlands, Poland, Portugal, Romania, Slovak Republic, Slovenia, Spain, Sweden and the United Kingdom. The zone EU-15 comprise the first 15 countries of the EU-28. The OECD zone includes all Member countries of the OECD i.e. Australia, Austria, Belgium, Canada, Chile, the Czech Republic, Denmark, Estonia, Finland, France, Germany, Greece, Hungary, Iceland, Ireland, Israel, Italy, Japan, Korea, Latvia, Lithuania, Luxembourg, Mexico, the Netherlands, New Zealand, Norway, Poland, Portugal, Slovak Republic, Slovenia, Spain, Sweden, Switzerland, Turkey, the United Kingdom, and the United States.

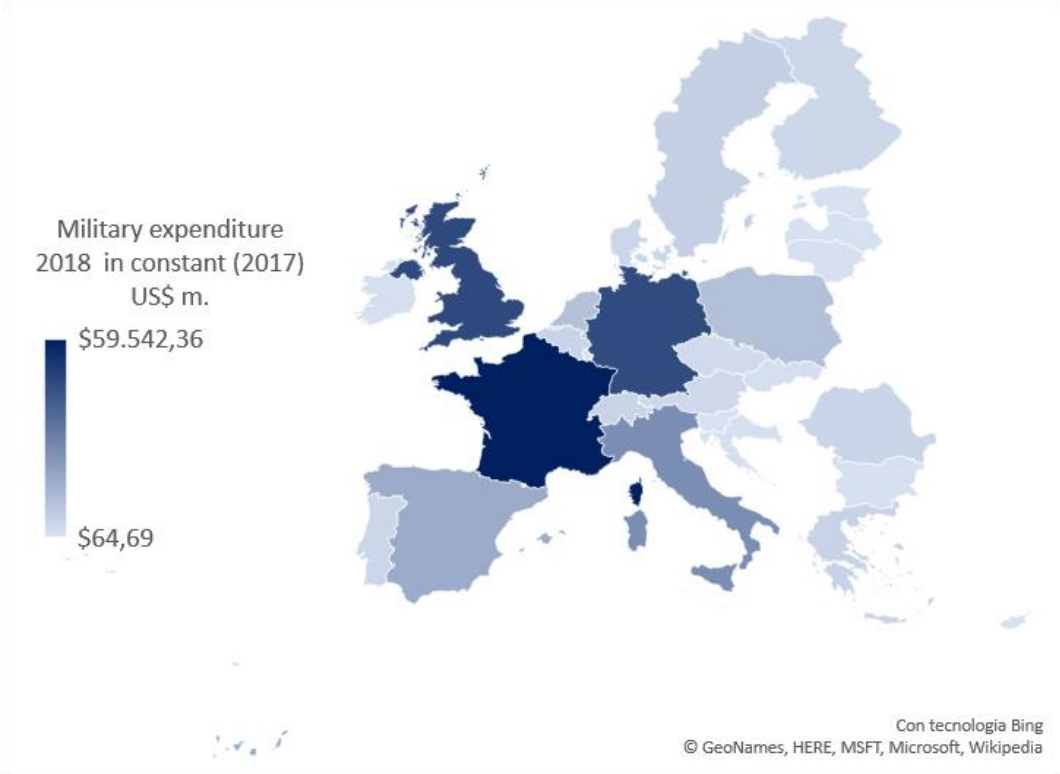


*Figure 2 - Distribution of military expenditure in European Union.*

| Country | Military expenditure 2018 in constant (2017) US$ m. | Percentage of 2018 military expenditure per EU MS related to total military expenditure in 2018 |
|---|---|---|
| France | $59.542,36 | 22,38% |
| United Kingdom | $46.883,23 | 17,62% |
| Germany | $46.191,81 | 17,36% |
| Italy | $26.082,40 | 9,80% |
| Spain | $17.038,59 | 6,40% |
| Poland | $10.748,89 | 4,04% |
| Netherlands | $10.534,91 | 3,96% |
| Sweden | $5.733,08 | 2,15% |
| Greece | $4.933,69 | 1,85% |
| Switzerland | $4.712,72 | 1,77% |
| Belgium | $4.613,73 | 1,73% |
| Romania | $4.257,63 | 1,60% |
| Denmark | $3.970,66 | 1,49% |
| Portugal | $3.968,59 | 1,49% |
| Finland | $3.615,01 | 1,36% |

| Country | Military expenditure 2018 in constant (2017) US$ m. | Percentage of 2018 military expenditure per EU MS related to total military expenditure in 2018 |
|---|---|---|
| Austria | $3.139,70 | 1,18% |
| Czechia | $2.445,64 | 0,92% |
| Slovakia | $1.185,97 | 0,45% |
| Ireland | $1.139,90 | 0,43% |
| Bulgaria | $1.015,03 | 0,38% |
| Lithuania | $955,98 | 0,36% |
| Croatia | $827,18 | 0,31% |
| Latvia | $629,22 | 0,24% |
| Estonia | $570,81 | 0,21% |
| Slovenia | $493,18 | 0,19% |
| Luxembourg | $392,65 | 0,15% |
| Cyprus | $359,97 | 0,14% |
| Malta | $64,69 | 0,02% |
| **Total military expenditure** | $266.047,23 | |

*Table 3 - Military expenditure in 2018 for each EU Member State as value in constant (2017) US$ and as percentage of the total.*

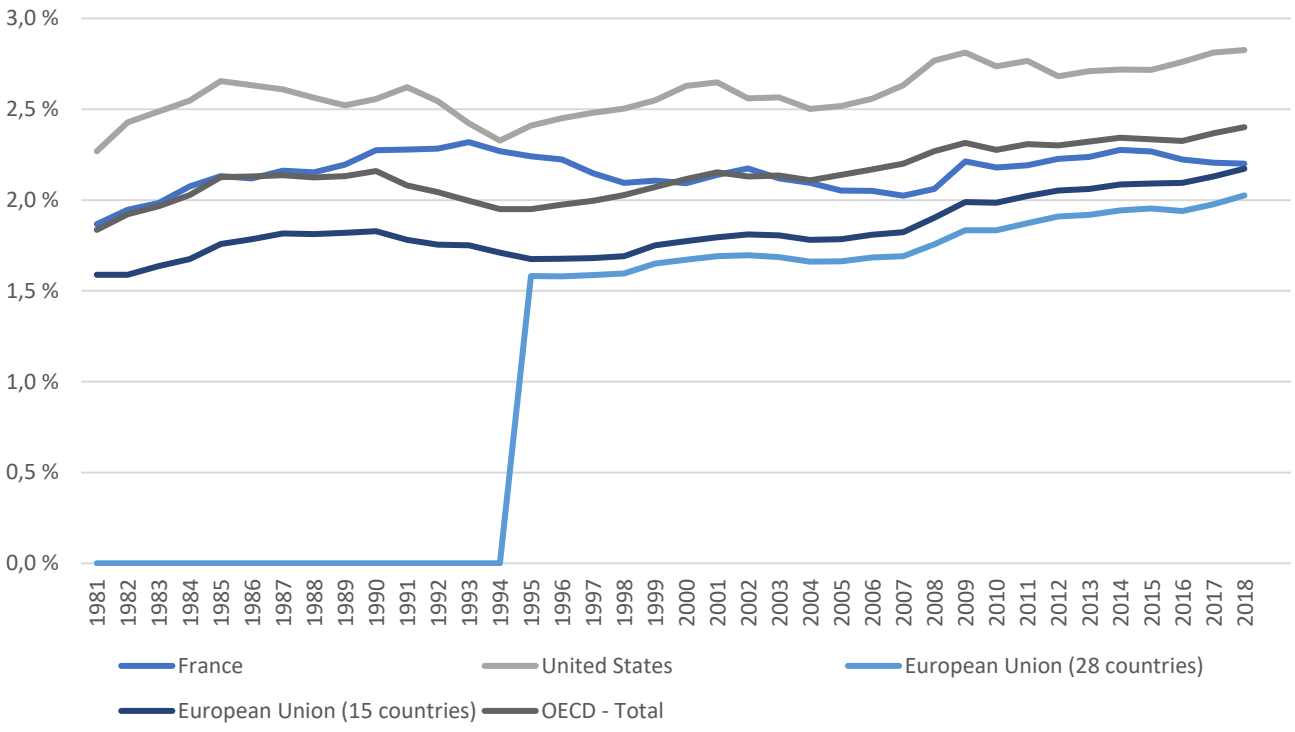


*Figure 3 - GERD as percentage of GDP from 1980 to 2018 in OECD countries, U.S., European Union and France.*

Moreover, since 2013, the European Commission has been encouraging industry and stakeholders to make the best use of existing EU programmes and tools. All designed to address skills gaps and to foster new skills, retraining, and reskilling to tackle the challenges of the sector. This was reiterated in the European defence action plan[3]. In 2018 the European Defence Skills Partnership was launched to help EU member states in sharing knowledge and best practices on skills and work together on the development and the implementation of solutions to handle the skills gaps. The activities includes platform, mapping of defence skills and best practices.

The EDSP includes industry, academia, authorities and innovation, research and vocational organisations, that cooperate in building skills for the European defence industry with the purpose to meet Europe's future security needs.

The industrial development of the last years requires re-skilling and up-skilling for the actual and future workforce to ensure the capabilities necessary to operate in a great range of advanced technological areas.

"To ensure success, the European Commission developed a comprehensive approach on skills involving all supply chain players, not only prime contractors but also SMEs and mid-cap companies. A number of instruments are considered to address skills at all the levels: regional, national and EU. It does this through the Blueprint for Sectoral Cooperation on Skills initiative, launched with the New Skills Agenda for Europe in 2016 and supported by the European Defence Action Plan"[4].

### 2.2.2 Analysis of the Defence Industrial Base (DIB)

The public commitment in Defence influences competition and innovation in the DIB.

Since the DIB develops, produces and provides goods and services for the Military Department of a State, in each Nation there is a solid group of core contractors and various suppliers at the lower levels of the supply chain (Hartley, K. et al., 2019). As a meaning of example, "the French Defence Technological and Industrial Base (DTIB) is structured around a solid core group of suppliers, consisting of eight top class contractors, engine manufacturers and suppliers: Airbus Group, Arquus, Dassault Aviation, MBDA, Naval Group, Nexter, Safran and Thales. This situation is the result of Government policy decisions dating back to the 1960s and adaptations of industry to its environment" (Hartley, K. et al., 2019). The Government supports its DIB and it is also its main consumer. As a result, the Defence Industry is shaped on the National policy and financial decisions.

[3] https://ec.europa.eu/growth/sectors/defence/skills_en
[4] https://eudsp.eu/practical.asp?event_id=4370&page_id=9614

With the purpose to give evidence of this point, it is possible to analyse the SIPRI TOP 100 (SIPRI, 2019)[5].

Firms in SIPRI TOP 100 (SIPRI, 2019) can be classified in relation to the main operative sector, i.e. Defence and/or civil, looking at their arms sales as a percentage of their total sales, namely *AS/TS*. During the last decades, as presented the Figure 4, most of the major firms in Defence industry shift towards a mix production, since there are more dual firm than pure firms in the SIPRI TOP 100 (SIPRI, 2019). Then, considering the total amount, the arms sales covers the 33% of the total sales of the industry in 2018 and the 18% in 2002, proving a greater activity in civil market.

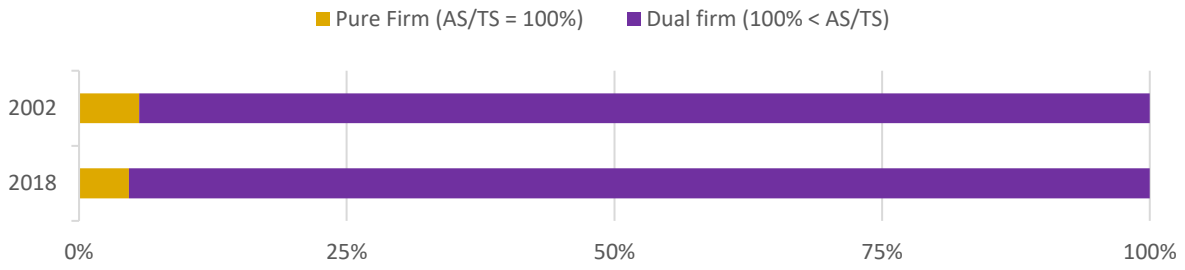


*Figure 4 - Comparison between the number of pure firms and dual firms in SIPRI TOP 100 [13] in 2002 and in 2018 as percentage of the total number of firms in SIPRI TOP 100 [13].*

The duality tendency is the effect of the reduction of public military expenditure that each Nation experienced after the Cold War. In U.S. "in 1993, Secretary of Defense Aspin and Deputy Secretary Perry concluded that some industrial consolidation was necessary and announced this to executives from major defense companies at a Pentagon dinner. The main message was that the major defense players needed to consolidate to survive and the Defense Department would facilitate the process by offering financial incentives and advocating consolidations in the event of antitrust challenges. The audience was receptive and as Norman Augustine (Martin Marietta CEO at the time) put it later: «You weren't going to survive unless you were willing to combine. So, there was not much of a choice»" (Hartley, K. et al., 2019).

The numbers of firms within each of the 20 different countries included in SIPRI TOP 100 (SIPRI, 2019) are presented in the Table 4, and the distribution of the market share among firms in SIPRI TOP 100 (SIPRI, 2019) is shown in the Figure 6, where the names of the firms with a market share greater than 3% (corresponding to a cumulative market share greater than 60%) and the Italian firms[6] are highlighted. These outcomes confirm the dominant position of the U.S. In fact, almost half of the firms in SIPRI TOP 100 (SIPRI, 2019) are American and as

[5] SIPRI TOP 100 derives from the SIPRI Arms Industry Database, that contains information on arms-producing and military services and is based on data from OECD as well as open sources, such as company annual reports and articles in journals and newspapers. SIPRI TOP 100 is updated every year since 2002.

[6] Leonardo and Fincantieri place respectively at the 8$^{th}$ and 50$^{th}$ position in the SIPRI TOP 100 in 2018 with a market share of 1,1% and 0,5%.

well the group of firms that gains the most part of the sales (General Electric, Boeing, United Technologies Corp., Lockheed Martin Corp. and Honeywell International), then there are also Trans-European firms (Airbus Group), German firms (ThyssenKrupp) and Japanese firms (Mitsubishi Electric Corp.). It is also notable that those companies (i.e. the ones with the higher market share) are all dual firms, proving the importance of the duality tendency.

| | **Number of firms in SIPRI TOP 100 [13]** | |
|---|---|---|
| **Country** | **2018** | **2002** |
| United States | 47 | 46 |
| Russia | 10 | 4 |
| United Kingdom | 10 | 13 |
| France | 6 | 9 |
| Japan | 6 | 6 |
| Germany | 4 | 8 |
| India | 3 | 3 |
| Israel | 3 | 5 |
| South Korea | 3 | 2 |
| Italy | 2 | 5 |
| Trans-European | 2 | 2 |
| Turkey | 2 | |
| Australia | 1 | 1 |
| Canada | 1 | 2 |
| Poland | 1 | |
| Singapore | 1 | 1 |
| Spain | 1 | 2 |
| Sweden | 1 | 1 |
| Switzerland | 1 | 1 |
| Ukraine | 1 | |
| Norway | | 1 |

*Table 4 - Number of firms per country in SIPRI TOP 100.*

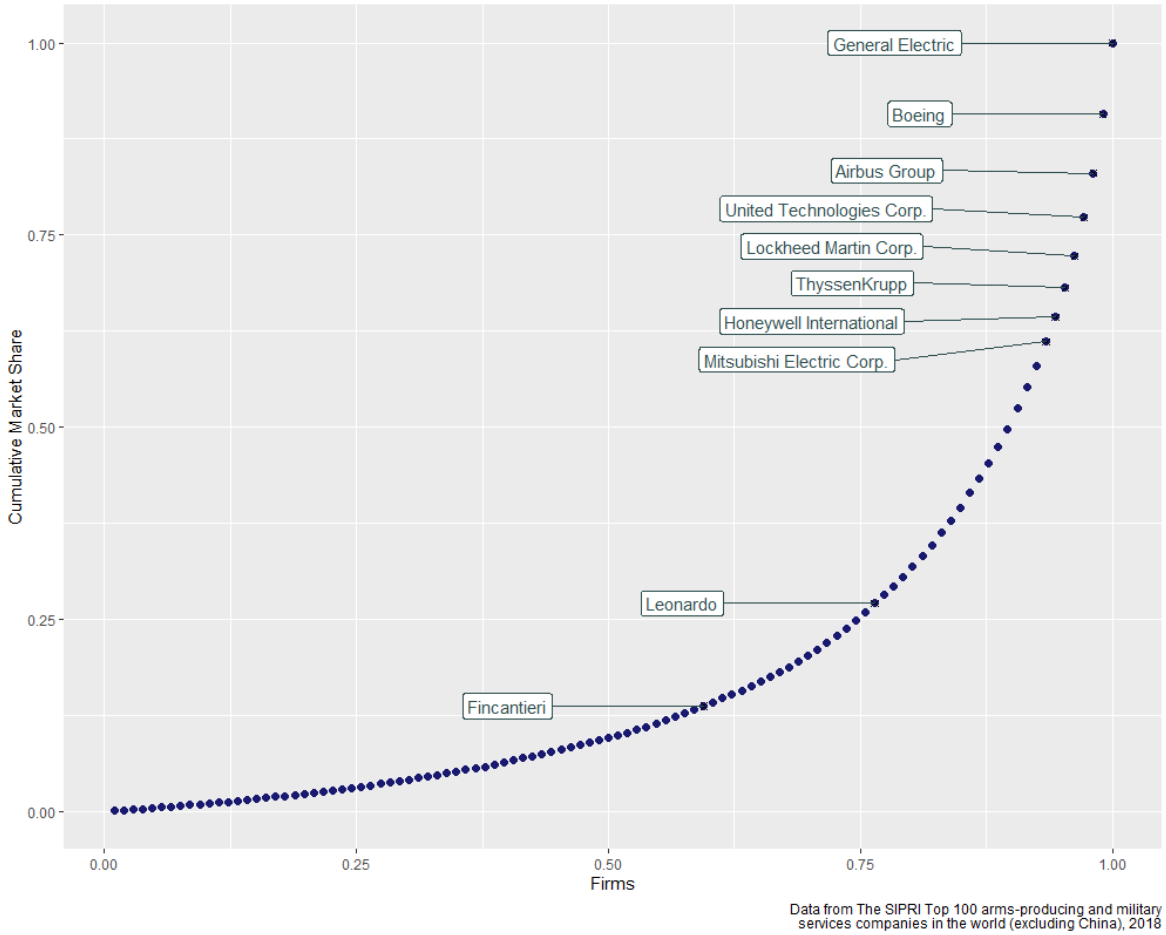


*Figure 5 - Distribution of the market share among firms in SIPRI TOP 100 in (2018).*

Moreover, the paradigm of unilateral and linear technology transfer from military to civilian, typical of the period from the 1940s to the 1980s, has been overcome by a circular approach in which the multiplicity of actors and purposes pushes an integration (European Commission, 2008).

In fact 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. In the context of Defence to give evidence of the complexity increase there are fighter aircraft (combination of knowledge from engines, electronics, weapon-system, structural design, material) or the massive use of ICT in weapon-system (Belin, J. et al., 2019)

In the last years, the number of dual technologies is increasing, especially in the field of Information Technology (IT), as a meaning of example but not limited to we can consider the advanced sensors that allows the real-time information gathering and sharing, or the tracing systems based on the Global Positioning Systems (GPS).

Traditionally in Europe military research and civil research have been considered as two distinct field, but the emerging technologies, especially in the field of IT and cybersecurity, reshaped the boundaries of civil and defence purpose filling the gap between civil and military and activating new synergies also involving more than one EU member states.

The technological domains under analysis in the ASSETs+ project, i.e. Artificial Intelligence, Robotics and Autonomous Systems, C4ISTAR and Cybersecurity, are related to the area of dual technologies, therefore it is necessary a constant supervision of the evolution of these most promising research areas in order to gain a competitive advantage in the global panorama both from the pure technical point of view and from the perspective of skills and knowledge necessary to handle correctly those technological development.

## 2.3 Technological Scope (concept)

The analysis on the evolution in the three technological domains (i.e Robotics, AI and autonomous systems, C4ISTAR, Cybersecurity), their impact on Defence sector and how the technologies could be applied, executed in the task T1.2 "Technology mapping", lead to the identification of 97 technologies and 59 defence-related application.

This paragraph contains: the domains definitions, the applications list with their descriptions for each domain, the map of the technologies classification with references to their maturity and level of abstraction, and finally the relevance matrix to link the technologies and the defence-related applications

### 2.3.1 Domains definitions

The three technological macro-areas are following defined.

**Robotics, artificial intelligence (AI) and autonomous-systems**: Robotics is an interdisciplinary sector of science and engineering dedicated to the design, construction and use of robots. The goal of robotics is to design intelligent machines that can help people in their daily lives, improve production processes and ensure safety. Robotics is a multidisciplinary science that encompasses the areas of computer science, mathematics, physics, mechanics, mechanical engineering, industrial engineering, electrical engineering, computer engineering, computer science, materials science, manufacturing engineering, automation and control, electronics, cybernetics and artificial intelligence, among others. Robotics is a unique combination of many scientific disciplines, whose fields of applications are broadening more and more, according to the scientific and technological achievements (Manseur, R., 1997 and Veruggio, G. et al., 2006). Artificial Intelligence is an area of study in the field of computer science. Artificial intelligence is concerned with the development of computers able to engage in human-like thought processes such as learning, reasoning, and self-correction (Kok, Joost N. et al., 2009). The autonomous-systems, that are devices or a softwares capable of perception, analysis and manipulation of its environment without or with limited human assistance. An autonomous-system is a device that

receives information through sensors and responds appropriately to carry out its mission all without direct human intervention (Stover, J. A. et al., 1992).

**C4ISTAR**: C4ISTAR stands for Command, Control, Communication, Computer, Information/Intelligence, Surveillance, Target Acquisition, and Reconnaissance. It indicates systems, structure, processes and all entities involved in missions and in military daily operations. It includes applications related to military operations, sensor systems, as well information technologies and telecommunications, tools and devices that create situational awareness (also known as Common Operational Picture – COP) and support decision making, information sharing and data fusion, promoting interoperability and integration during actions in the context of network-centric-warfare.

**Cybersecurity**: Cybersecurity involves a great set of techniques and methods for the protection of systems, as well as devices and networks, against damages towards availability, integrity, authentication, confidentiality, and non-repudiation. All systems, devices and networks should be available when required; data should remain inalterable at any point (integrity); identities should be verified prior to allowing access (authentication); authorized parties should be the only ones able to access protected resources (confidentiality); and a proof of sender's identity avoids the sender to deny a particular action or transmitted data (non-repudiation). Though the goal of cybersecurity is the same in all scenarios, protection measures should be aligned with each particular case, requiring experts of different fields working together in search of a common goal.

### 2.3.2 Applications of robotics, AI & autonomous-system domain

The number of applications identified in this domain of knowledge related to defence area is 26. The complete list of the robotics, AI and autonomous-systems applications is the following.

- **Aeronautics**: a science of designing, building, operating aircraft and science of flight Military aircraft allow logistic deliveries to forward bases, transporting air transport (cargo and soldiers), and take part in rescue operations during a national disaster. Military aviation includes transport, warships and fixed wing aircraft, rotary aircraft (RWA) and unmanned aerial vehicles (UAVs). (Biswas, K., 2019).
- **Anomaly detection:** refers to the problem of finding patterns in data that do not conform to expected behavior. (Chandola et al., 2009)
- **Assignment**: An optimization process of assigning items from one category with certain attributes to the other items from other categories in order to achieve desired results. (Burkard et al., 2012 and Munkres, J., 1957)
- **Coverage**: May refer to planning and optimizing the coverage effects of a particular area or group of things e.g. satellite coverage, artillery coverage, sensor coverage. (Longman dictionary and Cortes, J. et al., 2004)

- **Combat simulation**: Representations of military operations using gaming and calculation, with or without man-in-the-loop for training, analysis, and research. (Robinson et al., 1984)
- **Cyber resilience:** the ability to continuously deliver the intended outcome despite adverse cyber events. (Björck, F. et al., 2015)
- **Cyber security:** The body of technologies, processes, practices and response and mitigation measures designed to protect networks, computers, programs and data from attack, damage or unauthorized access so as to ensure confidentiality, integrity and availability. (Public Safety Canada. 2010 and Craigen, D. et al. 2014)
- **Fighter aircrafts**: military vehicle (plane) provide control over the necessary airspace by driving away or destroying an enemy aircraft. (Encyclopedia Britannica) Important issues here are designing, manufacturing, maintenance, reliability, safety.
- **Land armours**: an armored motor vehicle, usually armed with a cannon or machine guns. The main purpose of most armored cars was reconnaissance, less often combat. (Medlin, R. C., 2001). Important issues here are designing, manufacturing, testing, endurance, durability.
- **Military vehicle manufacturing:** industry that makes products from raw materials by the use of manual labour or machinery and that is usually carried out systematically with a division of labour. In a more limited sense, manufacturing denotes the fabrication or assembly of components into finished products on a fairly large scale. (Harris, Charles E. et al., 2002 and Britannica) The topics connected with military vehicles manufacturing, additional to manufacturing processes of other kind of products, are among others: data protection, special contracts with suppliers, concessions.
- **Missile**: an object (such as a weapon) thrown or projected usually so as to strike something at a distance. (Merriam-Webster's dictionary) Important issues here are missile designing, missile manufacturing, missile testing, missile reliability, missile control.
- **Mission control**: Mission control is a tool allowing for mission execution, supervision and mission parameters adjustment using human-machine interface. (J. Alves et al., 2006)
- **Mission planning**: Mission planning is a process of mission analysis that details required courses of action by specifying a sequence of tasks, defining resource-to-task allocation, and a timeline for all task activities. (G. M. Levchuk, 2002)
- **Naval**: fleet of ships whose task is to defend the interests of the state in maritime areas. In naval warfare, military aircraft play a significant role to detect and neutralize submarines and warships to keep the seacoast free from enemy attack. (Biswas, K., 2019) Important issues here are, among others: ships and equipment designing, manufacturing, communication, cybersecurity, object detection, fully integrating manned/unmanned systems, surface forces, submarine forces, naval aviation, naval special forces, coastal defence forces, planning, execution, and sustainment of major

naval/joint operations and maritime/littoral campaigns, steam and nuclear propulsion, internal combustion engine, submarine, airplane, mine, torpedo and missiles, undersea cable, wireless telegraphy, radio. (Smith, M. B., 2014; Haico te Kulve, H. et al., 2010 and Andrew Forbes 2015)

- **Path planning:** In robotics, path planning concerns problems such as how to move a robot from one point to another point. In artificial intelligence, path planning means a search for a sequence of logical actions that transform an initial robot state into a desired goal state. (DuchoĖ, František, et al., 2014)
- **Reconnaissance**: An exploratory survey to gain information in the enemy territory. [42]
- **Rescue**: A recovery of isolated personnel who are specifically designated as hostages or in danger. (Merriam-Webster's dictionary)
- **Routing**: An optimization process of assigning the specific routes from starting point to the desired destination while satisfying a set of requirements. It can be applied to vehicles and data in telecommunication networks. (Tarantilis C., 2008 and Ash, Gerald, 1997)
- **Scheduling**: A procedural planning that indicates the time and sequence of each operation. It deals with the allocation of resources to tasks over given time periods and its goal is to optimize one or more objectives. (Merriam-Webster's dictionary and Michael Pinedo, 2002)
- **Space technologies:** technology developed by space science or the aerospace industry for use in spaceflight, satellites, or space exploration. (Wikipedia) The current and future technologies can be connected with the following issues: launch system, reusable launch system, rocket engines, non-rocket space launched, space stations, satellites (remote sensing satellites, global positioning satellites, scientific research satellites, communication satellites, meteorological satellites, solar power satellites), satellites and cyberattack, photonics in space, etc. (Razani, M., 2018).
- **Surveillance**: The systematic observation of aerospace, cyberspace, surface, or subsurface areas, places, persons, or things by visual, aural, electronic, photographic, or other means. (DOD Dictionary of Military and Associated Terms)
- **Target tracking**: The target tracking objective is to collect sensor data from a field of view containing one or more potential targets of interest and to then partition the sensor data into sets of observations, or tracks, that are produced by the same sources. Once tracks are formed and confirmed (so that background and other false targets are reduced), the number of targets can be estimated and quantities, such as target velocity, future predicted position, and target classification characteristics, can be computed for each track. (Blackman, S. et al., 1992)
- **Trajectory tracking:** the problem of stabilizing the state, or an output function of the state, to a desired reference value, possibly time varying. So defined the trajectory tracking problem incorporates most of the problems addressed in the control literature: output feedback regulation, asymptotic stabilization of a fixed-point and, more generally,

of admissible non-stationary trajectories, practical stabilization of general trajectories. (Morin et al., 2004)

- **Underwater**: machines, systems, vehicles working under the water surface. Underwater vision systems (used in autonomous underwater vehicles) enable positioning and maintenance of stations, navigation and mosaic image of the seabed. Underwater vehicles include autonomous underwater vehicles (AUV), underwater gliders, unmanned underwater vehicles (UUV). (Nagahdaripour, S. et al., 1998; Horgan, J. et al., 2006 and Bogue, R., 2015)
- **Satellites**: a manufactured object or vehicle intended to orbit the earth, the moon, or another celestial body. They enable tele transmission of radio and television signals between ground stations. Currently, satellite operations are performed by robots that are semi-automatic and require monitoring and control by ground teams. In the future, it is planned to use unmanned orbital robots. (Barba, E. et al., 2020; García, J. et al., 2019 and Merriam-Webster's dictionary)
- **Weapons**: is a tool used to injure, defeat, or destroy an enemy / opponent. In the military industry, machine guns, machine pistols etc. and biological, chemical and nuclear weapons can be distinguished. (Swyter, H., 1970) Important issues here are weapon designing, weapon manufacturing, weapon testing, weapon reliability.

### 2.3.3 Applications of C4ISTAR domain

The identified potential defence applications related to C4ISTAR domain are 25 and the list has been generating by selecting applications based on their occurrence in a set of domain documents and the trend in the patents database related with C4ISTAR, as explained in the document R1.1 "Strategy Specification". The list of the C4ISTAR applications with a brief description is the following.

- **Authentication**: Authentication is a security measure designed to protect a communication system against acceptance of a fraudulent transmission or simulation by establishing the validity of a transmission, message, or originator. This process is used to identify individuals and verifying their identity and eligibility to receive specific categories of information. (White, F. E., 1991)
- **Command**: Command includes the authority and responsibility for effectively using available resources and for planning the employment, organizing, directing, coordinating and controlling military forces for the accomplishment of assigned missions establishing rules and constraints; and monitoring and assessing the situation and progress. The exercise of these functions requires a lawful authority that a commander in the military service exercises over subordinates by virtue of rank or assignment. (White, F. E., 1991 and Alberts, D. S., 2010)
- **Communication**: Communication is the transfer of intelligence, knowledge or information according to agreed conventions. (NATOterm)

- **Control**: Control refers to structures and processes to manage the mission problem in order to minimize the risk of not achieving a satisfactory solution. The concept embraces: the continuous acquisition, fusion, review, representation, analysis, and assessment of information on the situation; issuing the commander's plan; tasking of forces; operational planning; organizing and maintaining cooperation by all forces and all forms of support. It is related also to exert influence over an entity, process, object or area to establish, maintain or prevent a specific situation or event. (Alberts, D. S., 2010)
- **Data Analysis**: Data Analysis is a process of inspecting, cleansing, transforming and modeling data with the goal of discovering useful information, informing conclusion and supporting decision-making. (Xia, B. S. et al., 2015)
- **Data Fusion**: Data Fusion is a process dealing with the association, correlation, and combination of data and information from single and multiple sources to achieve refined position and identity estimates, and complete and timely assessments of situations and threats as well as their significance. (White, F. E., 1991)
- **Data Processing**: Data Processing is the process to organise data for the analysis. These may involve placing data into rows and columns in a table format for further analysis, such as within a spreadsheet or statistical software. (Schutt, R. 2013)
- **Decision Making**: Decision Making is the process of choosing among several alternative possibilities. (Brockmann, E. N. et al., 2016)
- **Encryption**: Encryption is the transformation of data, for the purpose of privacy, into an unreadable format until reformatted with a decryption key, so that only authorized individuals can read it. (fieldtechnologiesonline)
- **Identification**: Identification is the process of determining the friendly or hostile character of an unknown detected contact. In arms control, the process of determining which nation is responsible for the detected violations of any arms control measure. In combat operations, discrimination between recognizable objects as being friendly or enemy, or the name that belongs to the object as a member of a class. (White, F. E., 1991)
- **Imagery**: Imagery is the collection by visual photography, infrared sensors, lasers, electro optics and radar sensors such as synthetic aperture radar wherein images of objects are reproduced optically or electronically on film, electronic display devices or other media. (White, F. E., 1991)
- **Information processing**: Information processing is the change of information in any manner detectable by an observer. It concerns with gathering, manipulating, storing, retrieving, and classifying recorded information. (Denning, P. J. et al., 2012)
- **Information Sharing**: Information Sharing is the act of passing information from one to another.

- **Intelligence**: Intelligence refers collectively to the functions, activities and organizations which are involved in the process of planning, gathering, and analyzing information of potential value to decision makers and to the production of intelligence as defined above. (White, F. E., 1991)
- **Logistic**: Logistic is the process of planning and organizing to make sure that resources are in the places where they are needed, so that an activity or a process happens effectively.
- **Messaging**: Messaging is the process of sending someone a communication in writing, in speech, or by signals.
- **Mission**: Mission is an important official job that a person or a group of people are sent somewhere to do. It is related to a specific task with which a person or a group is charged.
- **Monitoring**: Monitoring is a continuous assessment of programmes based on early detailed information on the progress or delay of the ongoing assessed activities. (United Nations Development Programme)
- **Navigation**: Navigation is the method of determining position, course, direction and distance traveled.
- **Planning**: Planning is the establishment of goals, policies, and procedures in deciding how to do something to achieve the desired goal.
- **Positioning**: Positioning is the process related to determining the position of a vehicle or person on the surface of the Earth. (Tetley, L. et al., 2007)
- **Programming**: Programming is the process of translating the system specifications prepared during the design stage into program code. (Laudon, K. C. et al., 2011)
- **Reconnaissance**: Reconnaissance is a mission undertaken to obtain, by visual observation or other detection methods, information about the activities and resources of an enemy or potential enemy; or to secure data concerning the meteorological, hydrographic or geographic characteristics of a particular area. Also known as RECCE or RECON. (White, F. E., 1991)
- **Remote control**: Remote control is a process or a system for controlling something (such as a machine or vehicle) from a distance, by using electrical or radio signals.
- **Simulation**: Simulation is an approximate imitation of the operation of a process or system, that represents its operation over time. (Banks, J. et al., 2001)
- **Surveillance**: Surveillance is the systematic observation of aerospace, surface, subsurface areas, places, persons, or things by visual, electronic, photographic, or other means. (White, F. E., 1991)
- **Target Acquisition**: Target acquisition is the detection, identification and location of a target in sufficient detail to permit the effective employment of weapons. It is related to target analysis, as an examination of potential targets to determine military

importance, priority of attack, and weapons required to obtain a desired level of damage or casualties. (White, F. E., 1991)

2.3.4 Applications of Cybersecurity domain

The number of applications identified in this domain of knowledge related to defence area is 8. The complete list of the cybersecurity applications is the following.

- **Defense industrial base (DIB) collaboration**: Defense industrial base collaboration provides increased assurance to the Defence Department that a DIB contractor can adequately protect contract and controlled information at a level commensurate with the risk, accounting for information flow down to its subcontractors in a multi-tier supply chain. (Cybersecurity maturity model certification)
- **Cyber security awareness and training**: Cyber security awareness and training is the use of training platform to address the cybersecurity weakest link, the user; providing enhanced guidance for conduct and proper use of information technology by military personnel, in order to increase operational efficiency.
- **Operations Security (OPSEC)**: Operations security is a process to help to identify those actions that can be observed or collected by adversaries, determine indicators that adversaries might obtain and interpret to derive critical information, and, if appropriate, select and execute OPSEC measures that eliminate or reduce risk to an acceptable level. (osti.gov)
- **Cyber Operations (CO)**: Cyber operations is the cyberspace capabilities whose main purpose is to attain the objectives in or through cyberspace. Cyber Operations can be further classified into Ciber Operation (OCO) and Defensive Operation (DCO). (Karamanetal, M., n.d.)
- **Military Information Support Operations (MISO)**: Military information support operations are the actions specifically concerned with the integrated employment of cyberspace information-related capabilities during military operations, to influence, disrupt, corrupt, or usurp the decision making of adversaries and potential adversaries while protecting friendly forces.
- **Command and Control Support**: Command and control support is the command & control decision support (Intelligence, Surveillance, Target Acquisition, Reconnaissance).
- **Secure Communication (COMSEC)**: Secure communication is used to protect both classified and unclassified traffic on military communications networks, including voice, video, and data. (doi.org)
- **Cyber electronic warfare activities (CEWA)**: Cyber electronic warfare activities merge cyber and electronic warfare in the same context to support, enable, protect,

and collect on capabilities operating within the electromagnetic spectrum (EMS), including cyberspace capabilities. (Karamanetal, M., n.d.)

It is worth noting that some of the identified technologies and/or applications are related to attack missions. Therefore, they will not be pursued to design the educational programmes, considering the scope of our project. However, they are cited in this report for the sake of completion.

For what concern the robotics, AI and autonomous systems domain, such attack-related applications include missiles, fighter aircrafts and weapons.

Regarding the cybersecurity domain, Open Source Intelligence (OSINT)/Private Intelligence (PRIVINT) and Penetration Testing/Red Teaming are two technologies that can be used for either offensive or defensive purposes. For example, OSINT/PRIVINT are often used to check what sensitive information about its own staff is publicly exposed to the enemy (thus, it can be viewed as a defensive technique). However, this technology can also be used to find out information about the enemy in the preparation of a military operation (thus, it can also be viewed as an offensive technique). OSINT only uses information publicly available (e.g., Facebook, etc.). As such, it can be considered non-intrusive.

The same applies to Penetration Testing/Red Teaming. Albeit intrusive, these technologies are often used to examine for security breaches in its own assets (e.g., data network, applications or computer systems), so they can be viewed as defensive technologies.

However, these technologies can also be used as the first step in an offensive operation, to gain control over the enemy's assets. As such, they can also be viewed as offensive technology. To sum up, those technologies can be viewed as defensive technologies, but they can well be also used in the first stage of an offensive operation.

### 2.3.5 Technologies Map

The following map describes the core technologies within the three domains under analysis, as identified in the task T1.2 "Technologies Mapping" by the WP1 team, considering their maturity and abstraction levels. The whole results can be found in the R1.2 "Technologies Roadmap".

The **maturity level** of a technology, the horizontal dimension of the map, is the achieved state of a specific technology in its evolution, considering the interest from research and industrial parties. A technology can be labelled as:

- *Outdated*: technologies that were relevant in the past but are now replaced with other technologies;
- *Emerging*: technologies that are starting to attract researchers and industries;

- *Mature*: technologies that have reached a high level of maturity in the research community but are not yet widely adopted in industry;
- *Established*: technologies that have been well documented and studied by the research community and that are widely adopted in industry.

The **abstraction level** of a technology, the vertical dimension of the map, is defined as the process of extracting the underlying structures, patterns, or properties of some objects, with the intention of generalizing these findings to a broader class of objects[7]. Therefore, based on this definition, a qualitative evaluation of the Abstraction Level is provided:

- *High*: less detailed technologies (e.g. an entire system);
- *Medium*: more detailed technologies (e.g. a group of components that constitute a finite element of the whole system);
- *Low*: specific technologies (e.g. a single part of a group component).

The technologies presented in the map in Figure 6 are related to all the three domains under analysis, therefore they are identified by a different colour: *pink* for the robotics, AI & autonomous-system domain, *blue* for the C4ISTAR domain and *yellow* for the Cybersecurity domain.

[7] https://en.wikipedia.org/wiki/Abstraction#In_mathematics

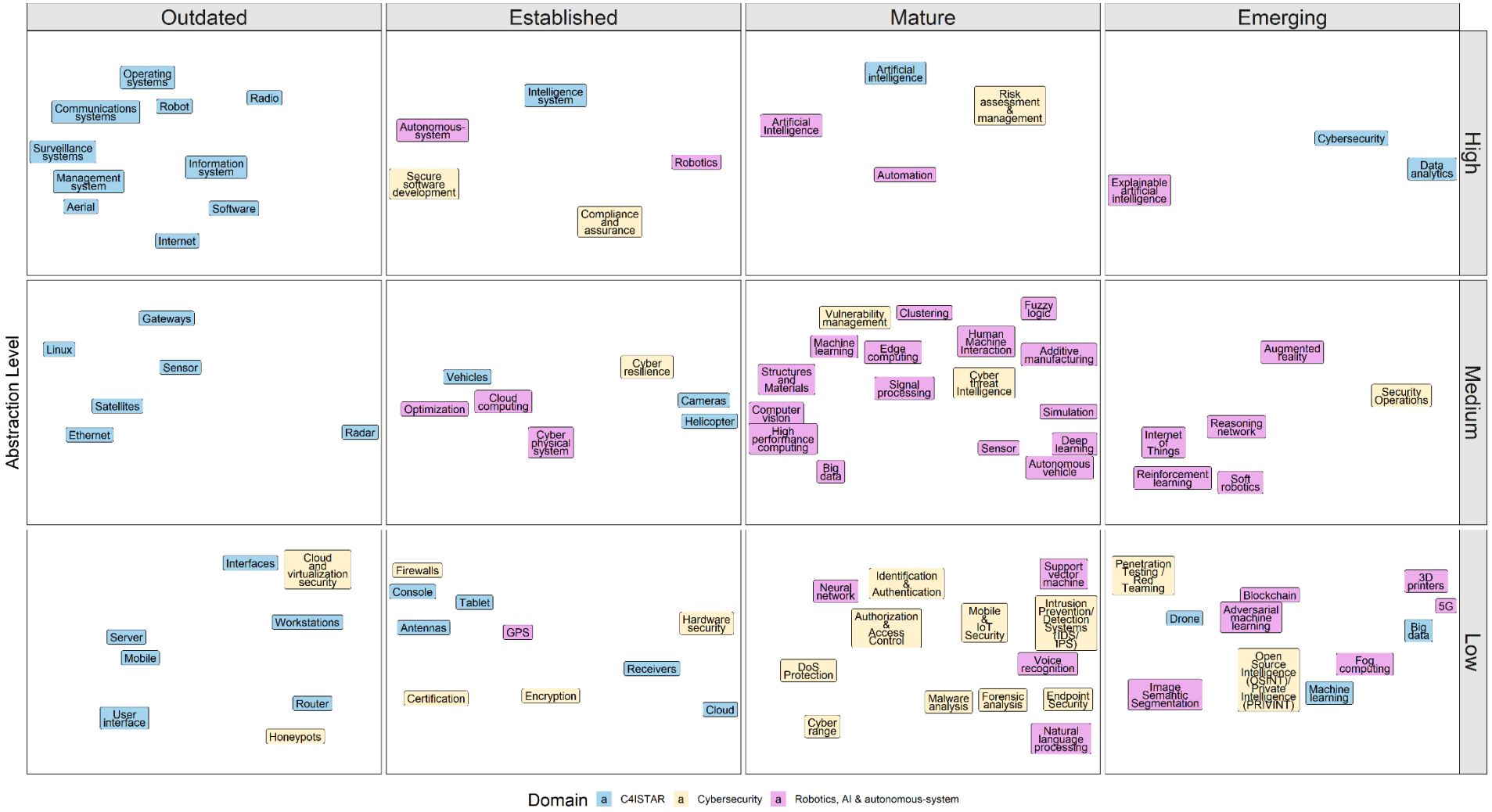


*Figure 6 - Technologies map for the robotics, AI & autonomous-system, the C4ISTAR and the Cybersecurity domains.*

## 2.4 Knowledge to master the Defence Technologies

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. Nowadays it is necessary finding and applying different policies to increase the sustainability and the capacity of the European defence industry. The analysis on the skills needs for the Defence Industry, executed in the task T1.3 "Emerging skills related to selected techs", leads to the identification of 172 skills and 181 job profiles.

The results can be found in the R1.3 "Skill Blueprint". This document describes the links between the identified emerging technologies and the skills to correctly exploit them in Defence. The following graphs describe the skills identified, classified in 3 categories with references on their degree of specialization, degree of knowledge and demand from labour market. All of these concepts are defined as following.

The category of **technical skills** is related to the skills required to correctly exploit a certain technology within a given defence application. The **Defence-related skills** encompass the skills connected to the knowledge, the use and the management of methods and procedures typical of the defence applications. The group of **transversal skills** includes the soft skills that are having an increasing importance in all the industries and also in defence.

The **degree of specialisation** represents how important the skill is for the relative job profile in the defence sector and it can be:

- *Low*: Commonly available and used; this is a skill/competence that is widely in all the sectors; it is fully transferable;
- *Medium*: Widely used by defence; this is a skill/competence that is used widely in defence and to an extent in the civil sector;
- *High*: Specialised for defence; this is a skill/competence that is used in the defence sector and requires an extensive background in defence engineering.

The **degree of knowledge** indicates the required level of a skill for the relative job profile to perform a defence-related job and it can be:

- *Low*: basic level of knowledge related to the specific skills to perform a set of tasks for the given job profile, so the job profile doesn't require a great expertise;
- *Medium*: intermediate level of knowledge related to the specific skills to perform a set of tasks for the given job profile, so the job profile requires a certain expertise;
- *High*: advanced level of knowledge related to the specific skills to perform a set of tasks for the given job profile, so the job profile requires a great expertise;

The **demand from labour market** indicates how much a skill is required for the given job profile, it can be:

- *Low*: the defence sector shows a lack of demand for a skill related to the given job profile;
- *Medium*: the defence sector demands for a skill related to the given job profile, but not extensively;
- *High*: the defence sector has a high demand for a skill related to the given job profile.

The skills classifications for each technological domain under analysis are presented in the graphs below. In particular, the Figure 7 includes the skills for the robotics, AI & autonomous-system domain, the Figure 8 presents the skills for the C4ISTAR domain and the Figure 9 describe the skills for the Cybersecurity domain. In these graphs, each bar represents the value of a given indicator related to a given skill.

The full list of skill with their original names and labels is provided in the Appendix 1.

Finally, the Figure 10 lists the defence-related skills connected with the three technological domains under analysis in the ASSETs+ project.

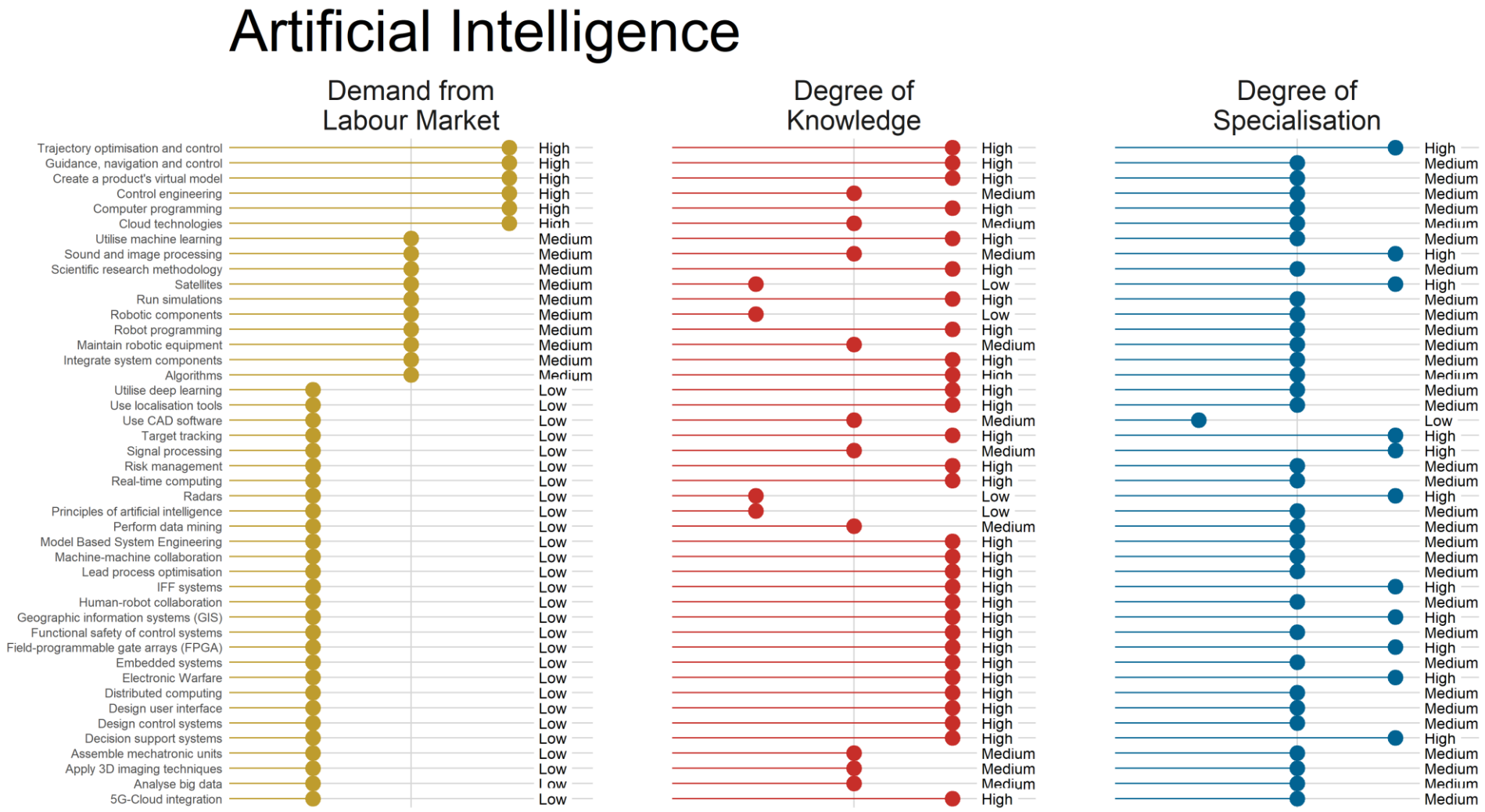


*Figure 7 - Skills classification for the robotics, AI & autonomous-system domain.*

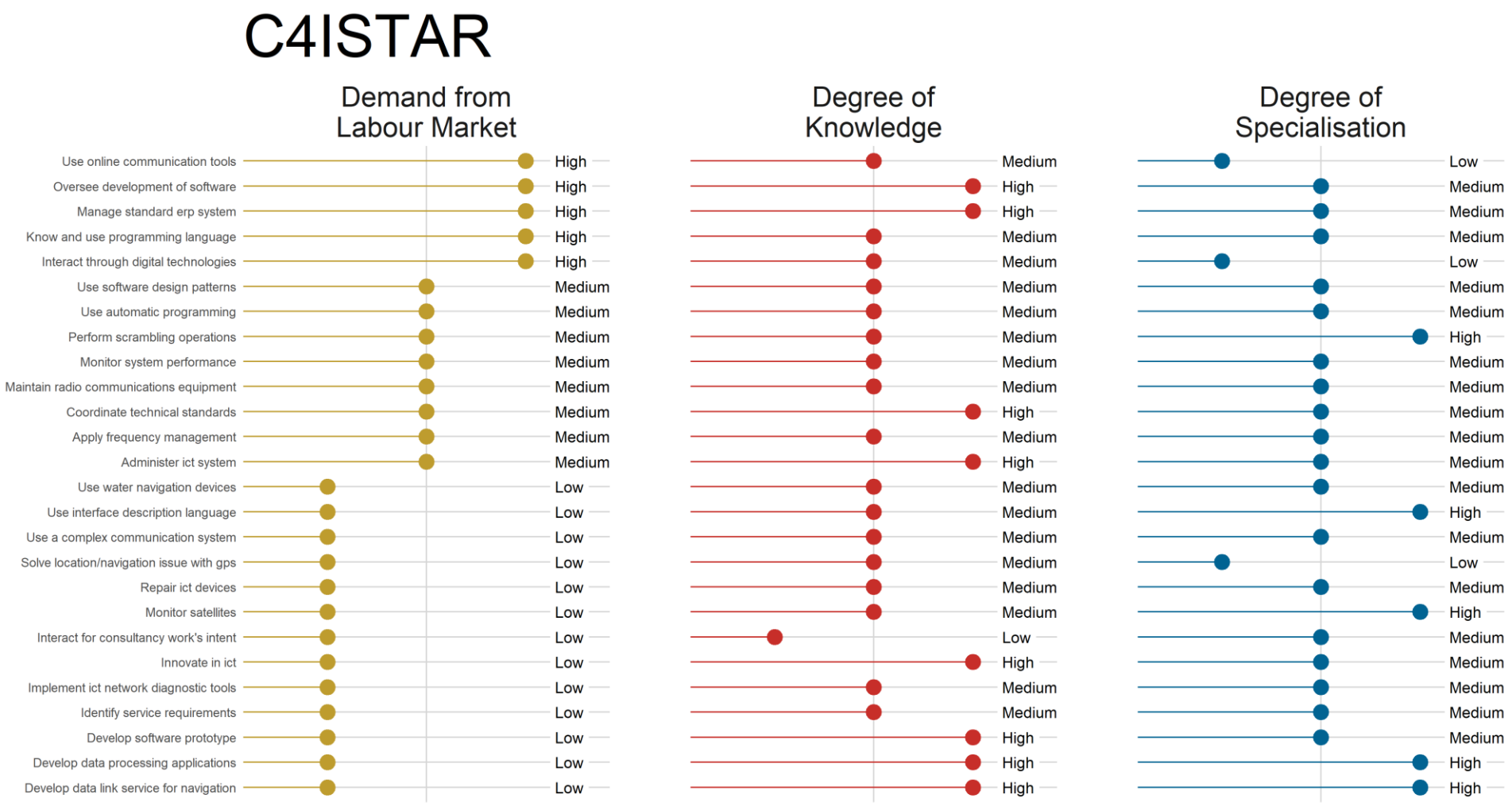


*Figure 8 - Skills classification for the C4ISTAR domain.*

# Cybersecurity

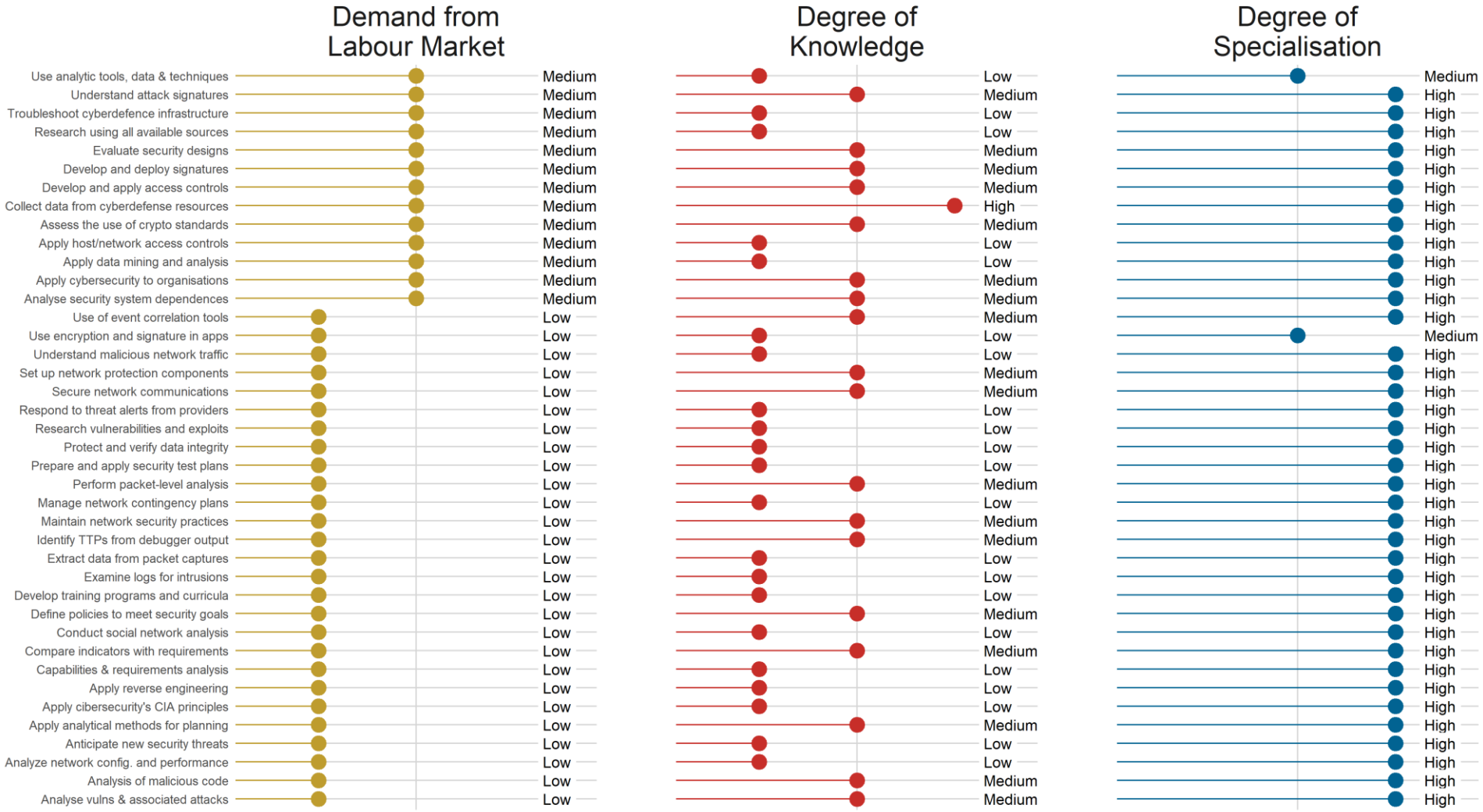


*Figure 9 - Skills classification for the Cybersecurity domain.*

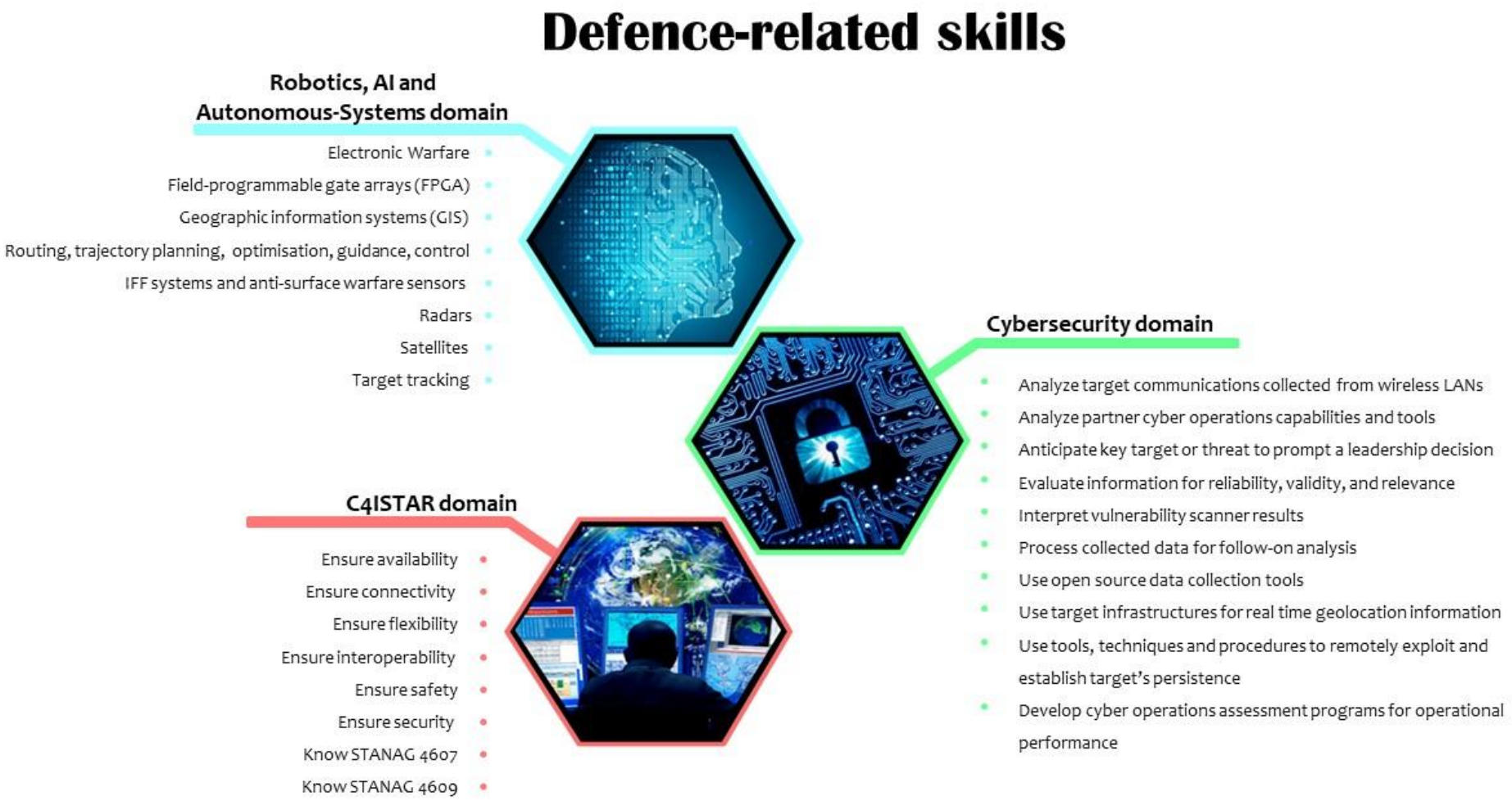


*Figure 10 - Defence-related skills for the three technological domains in analysis in the ASSETs+ project*

# 3. Conclusions

The problem facing the European Defence Industry is twofold: (i) its experiencing difficulty in finding the necessary skills in order to sustain its leadership, competitiveness and sustainability in the medium to longterm; (ii) aging staff and difficulties in engaging and keeping young professionals are preventing the sector from reshaping company capabilities and creating new, attractive job opportunities for talented workers of any age.

ASSETs+ project aspires to build a sustainable human resources supply chain which allows Defence sector companies to innovate by both attracting highly-skilled young workers and upskilling their employees thanks to customised, complementary education & training programmes addressing three main technologies: Robotics, artificial intelligence and autonomous-systems, C4ISTAR, and Cybersecurity aspects related to the first two.

The development of a Defence Body of Knowledge (BOK) with defence-specific topics for the different mentioned technologies is thus a key element for the exploitation strategy of the sector and it is strongly linked with both skills (demand and offer) and qualifications.

The ASSETs+ BOK, presented in this document, can be seen as a guidance document for the European Defence Sector, containing specific competences needed to master the technologies within the project scope.

ASSETs+ BOK is also intended to be a future reference for any person working for or on behalf of Defence sector bodies or organisations. In order to promote this continuous new skills acquisition, development and retention, the BOK will be updated every year.

# Appendix 1.

This appendix contains the full list of technical skill of the three technological domains under analysis with the original names and the updated labels.

| Domain | Skill | Label | Type of skill |
|---|---|---|---|
| Robotics, artificial intelligence (AI) and autonomous-systems | Algorithms | Algorithms | technical skill |
| Robotics, artificial intelligence (AI) and autonomous-systems | Analyse big data | Analyse big data | technical skill |
| Robotics, artificial intelligence (AI) and autonomous-systems | Apply 3D imaging techniques | Apply 3D imaging techniques | technical skill |
| Robotics, artificial intelligence (AI) and autonomous-systems | Assemble mechatronic units | Assemble mechatronic units | technical skill |
| Robotics, artificial intelligence (AI) and autonomous-systems | Cloud technologies | Cloud technologies | technical skill |
| Robotics, artificial intelligence (AI) and autonomous-systems | Computer programming (Python, C, C++, R, Java, MATLAB, Lisp, Prolog) | Computer programming | technical skill |
| Robotics, artificial intelligence (AI) and autonomous-systems | Control engineering | Control engineering | technical skill |
| Robotics, artificial intelligence (AI) and autonomous-systems | Create a product's virtual model | Create a product's virtual model | technical skill |
| Robotics, artificial intelligence (AI) and autonomous-systems | Decision support systems | Decision support systems | technical skill |
| Robotics, artificial intelligence (AI) and autonomous-systems | Design control systems | Design control systems | technical skill |
| Robotics, artificial intelligence (AI) and autonomous-systems | Design user interface | Design user interface | technical skill |
| Robotics, artificial intelligence (AI) and autonomous-systems | Distributed computing | Distributed computing | technical skill |
| Robotics, artificial intelligence (AI) and autonomous-systems | Electronic Warfare | Electronic Warfare | technical skill |
| Robotics, artificial intelligence (AI) and autonomous-systems | Embedded systems | Embedded systems | technical skill |
| Robotics, artificial intelligence (AI) and autonomous-systems | Field-programmable gate arrays (FPGA) | Field-programmable gate arrays (FPGA) | technical skill |
| Robotics, artificial intelligence (AI) and autonomous-systems | Functional safety of control systems | Functional safety of control systems | technical skill |
| Robotics, artificial intelligence (AI) and autonomous-systems | Geographic information systems (GIS) | Geographic information systems (GIS) | technical skill |
| Robotics, artificial intelligence (AI) and autonomous-systems | Guidance, navigation and control | Guidance, navigation and control | technical skill |
| Robotics, artificial intelligence (AI) and autonomous-systems | Human-robot collaboration | Human-robot collaboration | technical skill |
| Robotics, artificial intelligence (AI) and autonomous-systems | IFF systems and anti-surface warfare sensors | IFF systems | technical skill |
| Robotics, artificial intelligence (AI) and autonomous-systems | Integrate system components | Integrate system components | technical skill |
| Robotics, artificial intelligence (AI) and autonomous-systems | Integration of 5G services with Cloud Services | 5G-Cloud integration | technical skill |
| Robotics, artificial intelligence (AI) and autonomous-systems | Lead process optimisation | Lead process optimisation | technical skill |

| Domain | Skill | Label | Type of skill |
|---|---|---|---|
| Robotics, artificial intelligence (AI) and autonomous-systems | Machine-machine collaboration | Machine-machine collaboration | technical skill |
| Robotics, artificial intelligence (AI) and autonomous-systems | Maintain robotic equipment | Maintain robotic equipment | technical skill |
| Robotics, artificial intelligence (AI) and autonomous-systems | Model Based System Engineering | Model Based System Engineering | technical skill |
| Robotics, artificial intelligence (AI) and autonomous-systems | Perform data mining | Perform data mining | technical skill |
| Robotics, artificial intelligence (AI) and autonomous-systems | Principles of artificial intelligence | Principles of artificial intelligence | technical skill |
| Robotics, artificial intelligence (AI) and autonomous-systems | Radars | Radars | technical skill |
| Robotics, artificial intelligence (AI) and autonomous-systems | Real-time computing | Real-time computing | technical skill |
| Robotics, artificial intelligence (AI) and autonomous-systems | Risk management | Risk management | technical skill |
| Robotics, artificial intelligence (AI) and autonomous-systems | Robot programming | Robot programming | technical skill |
| Robotics, artificial intelligence (AI) and autonomous-systems | Robotic components | Robotic components | technical skill |
| Robotics, artificial intelligence (AI) and autonomous-systems | Routing, trajectory planning, optimisation, guidance and control | Trajectory optimisation and control | technical skill |
| Robotics, artificial intelligence (AI) and autonomous-systems | Run simulations | Run simulations | technical skill |
| Robotics, artificial intelligence (AI) and autonomous-systems | Satellites | Satellites | technical skill |
| Robotics, artificial intelligence (AI) and autonomous-systems | Scientific research methodology | Scientific research methodology | technical skill |
| Robotics, artificial intelligence (AI) and autonomous-systems | Signal processing | Signal processing | technical skill |
| Robotics, artificial intelligence (AI) and autonomous-systems | Target tracking | Target tracking | technical skill |
| Robotics, artificial intelligence (AI) and autonomous-systems | Use CAD software | Use CAD software | technical skill |
| Robotics, artificial intelligence (AI) and autonomous-systems | Use localisation tools | Use localisation tools | technical skill |
| Robotics, artificial intelligence (AI) and autonomous-systems | Using digital tools for processing sound and images | Sound and image processing | technical skill |
| Robotics, artificial intelligence (AI) and autonomous-systems | Utilise deep learning | Utilise deep learning | technical skill |
| Robotics, artificial intelligence (AI) and autonomous-systems | Utilise machine learning | Utilise machine learning | technical skill |
| C4ISTAR | administer ICT system | administer ICT system | technical skill |
| C4ISTAR | apply frequency management | apply frequency management | technical skill |
| C4ISTAR | coordinate technical standards for global interoperability | coordinate technical standards | technical skill |
| C4ISTAR | develop data link services for navigation purposes | develop data link service for navigation | technical skill |
| C4ISTAR | develop data processing applications | develop data processing applications | technical skill |

| Domain | Skill | Label | Type of skill |
|---|---|---|---|
| C4ISTAR | develop software prototype | develop software prototype | technical skill |
| C4ISTAR | identify service requirements | identify service requirements | technical skill |
| C4ISTAR | implement ICT network diagnostic tools | implement ICT network diagnostic tools | technical skill |
| C4ISTAR | innovate in ICT | innovate in ICT | technical skill |
| C4ISTAR | interact through digital technologies | interact through digital technologies | technical skill |
| C4ISTAR | interact with programmer on intention of consultancy work | Interact for consultancy work's intent | technical skill |
| C4ISTAR | know software interaction design and use programming language | know and use programming language | technical skill |
| C4ISTAR | maintain radio communications equipment | maintain radio communications equipment | technical skill |
| C4ISTAR | manage standard enterprise resource planning system | manage standard ERP system | technical skill |
| C4ISTAR | monitor satellites | monitor satellites | technical skill |
| C4ISTAR | monitor system performance | monitor system performance | technical skill |
| C4ISTAR | oversee development of software | oversee development of software | technical skill |
| C4ISTAR | perform scrambling operations | perform scrambling operations | technical skill |
| C4ISTAR | repair ICT devices | repair ICT devices | technical skill |
| C4ISTAR | solve location and navigation problems by using GPS tools | solve location/navigation issue with GPS | technical skill |
| C4ISTAR | use a complex communication system | use a complex communication system | technical skill |
| C4ISTAR | use automatic programming | use automatic programming | technical skill |
| C4ISTAR | use interface description language | use interface description language | technical skill |
| C4ISTAR | use online communication tools | use online communication tools | technical skill |
| C4ISTAR | use software design patterns | use software design patterns | technical skill |
| C4ISTAR | use water navigation devices | use water navigation devices | technical skill |
| Cybersecurity | skill in analyzing essential network data (e.g., router configuration files, routing protocols), network traffic capacity and performance characteristics | Analyze network config. and performance | technical skill |
| Cybersecurity | skill in applying analytical methods typically employed to support planning and to justify recommended | Apply analytical methods for planning | technical skill |

| Domain | Skill | Label | Type of skill |
|---|---|---|---|
| | strategies and courses of action | | |
| Cybersecurity | skill in applying confidentiality, integrity, and availability principles | Apply cibersecurity's CIA principles | technical skill |
| Cybersecurity | skill in applying host/network access controls (e.g., access control list) | Apply host/network access controls | technical skill |
| Cybersecurity | skill in assessing the application of cryptographic standards | Assess the use of crypto standards | technical skill |
| Cybersecurity | skill in collecting data from a variety of cyber defense resources | Collect data from cyberdefense resources | technical skill |
| Cybersecurity | skill in conducting capabilities and requirements analysis | Capabilities & requirements analysis | technical skill |
| Cybersecurity | skill in conducting research using all available sources (including deep web) | Research using all available sources | technical skill |
| Cybersecurity | skill in conducting social network analysis, buddy list analysis, and/or cookie analysis | Conduct social network analysis | technical skill |
| Cybersecurity | skill in conducting test event and secure test plan design (e. g. unit, integration, system, acceptance) | Prepare and apply security test plans | technical skill |
| Cybersecurity | skill in configuring and utilizing network protection components (e.g., firewalls, vpns, network intrusion detection systems) | Set up network protection components | technical skill |
| Cybersecurity | skill in creating policies that reflect system security objectives | Define policies to meet security goals | technical skill |
| Cybersecurity | skill in data mining techniques (e.g., searching file systems) and analysis | Apply data mining and analysis | technical skill |
| Cybersecurity | skill in deep analysis of captured malicious code (e.g., malware forensics) | Analysis of malicious code | technical skill |
| Cybersecurity | skill in determining how a security system should work (including its resilience and dependability capabilities) and how changes in conditions, operations, or the environment will affect these outcomes | Analyse security system dependences | technical skill |
| Cybersecurity | skill in developing and applying security system access controls | Develop and apply access controls | technical skill |
| Cybersecurity | skill in developing and deploying signatures | Develop and deploy signatures | technical skill |

| Domain | Skill | Label | Type of skill |
|---|---|---|---|
| Cybersecurity | skill in developing and executing technical training programs and curricula | Develop training programs and curricula | technical skill |
| Cybersecurity | skill in developing, testing, and implementing network infrastructure contingency and recovery plans | Manage network contingency plans | technical skill |
| Cybersecurity | skill in evaluating the adequacy of security designs | Evaluate security designs | technical skill |
| Cybersecurity | skill in extracting information from packet captures | Extract data from packet captures | technical skill |
| Cybersecurity | skill in implementing, maintaining, and improving established network security practices | Maintain network security practices | technical skill |
| Cybersecurity | skill in interpreting results of debugger to ascertain tactics, techniques, and procedures | Identify TTPs from debugger output | technical skill |
| Cybersecurity | skill in one-way hash functions (e.g., secure hash algorithm [sha], message digest algorithm [md5]) and verifying the integrity of all files | Protect and verify data integrity | technical skill |
| Cybersecurity | skill in performing packet-level analysis | Perform packet-level analysis | technical skill |
| Cybersecurity | skill in reading and interpreting signatures (e.g., snort) | Understand attack signatures | technical skill |
| Cybersecurity | skill in recognizing and categorizing types of vulnerabilities and associated attacks | Analyse vulns & associated attacks | technical skill |
| Cybersecurity | skill in recognizing and interpreting malicious network activity in traffic | Understand malicious network traffic | technical skill |
| Cybersecurity | skill in researching vulnerabilities and exploits utilized in traffic | Research vulnerabilities and exploits | technical skill |
| Cybersecurity | skill in reverse engineering (e.g., hex editing, binary packaging utilities, debugging, and strings analysis) to identify function and ownership of remote tools | Apply reverse engineering | technical skill |
| Cybersecurity | skill in reviewing logs to identify evidence of past intrusions | Examine logs for intrusions | technical skill |
| Cybersecurity | skill in securing network communications | Secure network communications | technical skill |
| Cybersecurity | skill in troubleshooting and diagnosing cyber defense infrastructure anomalies and work through resolution | Troubleshoot cyberdefence infrastructure | technical skill |

| Domain | Skill | Label | Type of skill |
|---|---|---|---|
| Cybersecurity | skill in using multiple analytic tools, databases, and techniques (e.g., analyst's notebook, a-space, anchory, m3, divergent/convergent thinking, link charts, matrices, etc.) | Use analytic tools, data & techniques | technical skill |
| Cybersecurity | skill in using public-key infrastructure (pki) encryption and digital signature capabilities into applications (e.g.,s/mime email, ssl traffic) | Use encryption and signature in apps | technical skill |
| Cybersecurity | skill in using security event correlation tools | Use of event correlation tools | technical skill |
| Cybersecurity | skill to anticipate new security threats | Anticipate new security threats | technical skill |
| Cybersecurity | skill to apply cybersecurity and privacy principles to organizational requirements (relevant to confidentiality, integrity, availability, authentication, non-repudiation) | Apply cybersecurity to organisations | technical skill |
| Cybersecurity | skill to compare indicators/observables with requirements | Compare indicators with requirements | technical skill |
| Cybersecurity | skill to respond and take local actions in response to threat sharing alerts from service providers | Respond to threat alerts from providers | technical skill |

# References

Alberts, D. S., Huber, R. K., & Moffat, J. (2010). NATO NEC C2 maturity model. OFFICE OF THE ASSISTANT SECRETARY OF DEFENSE WASHINGTON DC COMMAND AND CONTROL RESEARCH PROGRAM (CCRP).

Ash, Gerald (1997). Dynamic Routing in Telecommunication Networks. McGraw–Hill. ISBN 978-0-07-006414-0.

Banks, J., Carson, J. S., Nelson, B. L., & Nicol, D. M. (2001). Verification and validation of simulation models. Discrete-Event System Simulation, 3rd Edition, Prentice-Hall, Upper Saddle River (NJ), 367-397.

Barba, E., Lioon, A., Miller, C., & Khan, Y. M. (2020, April). Tele-robotic Interface Design in Context: A Case for Recursive Design. In Extended Abstracts of the 2020 CHI Conference on Human Factors in Computing Systems Extended Abstracts (pp. 1-8).

Belin, J., Guille, M., Lazaric, N., & Mérindol, V. (2019). Defense firms adapting to major changes in the French R&D funding system. *Defence and Peace Economics*, *30*(2), 142-158.

Biswas, K. (2019). Military Aviation Principles. In Military Engineering. IntechOpen.

Björck, Fredrik, et al. "Cyber resilience–fundamentals for a definition." New contributions in information systems and technologies. Springer, Cham, 2015. 311-316.

Blackman S., Popoli R. "Design and analysis of modern tracking systems." (1999).

Bogue, R. (2015). Underwater robots: a review of technologies and applications. Industrial Robot: An International Journal.

Brockmann, Erich N.; Anthony, William P. (December 2016). "Tacit knowledge and strategic decision making". Group & Organization Management. 27 (4): 436–455. doi:10.1177/1059601102238356.

Burkard, Rainer, Mauro Dell'Amico, and Silvano Martello. Assignment problems, revised reprint. Vol. 106. Siam, 2012, p.1

Chandola, Varun, Arindam Banerjee, and Vipin Kumar. "Anomaly detection: A survey." ACM computing surveys (CSUR) 41.3 (2009): 1-58.

Coverage In Longman dictionary https://www.ldoceonline.com/dictionary/coverage

Craigen, Dan, Nadia Diakun-Thibault, and Randy Purse. "Defining cybersecurity." Technology Innovation Management Review 4.10 (2014).

Cybersecurity maturity model certification (CMMC). Version 1.0 | January 30, 2020. Available at: https://www.acq.osd.mil/cmmc/draft.html

Denning, P. J., & Bell, T. (2012). The information paradox.

Differences Between OPSEC and Security Awareness. Available at: https://www.osti.gov/servlets/purl/1367112

DOD Dictionary of Military and Associated Terms, January 2020, https://www.jcs.mil/Portals/36/Documents/Doctrine/pubs/dictionary.pdf p.207

DuchoĖ, František, et al. "Path planning with modified a star algorithm for a mobile robot." Procedia Engineering 96 (2014): 59-69.

European Commission (2008). A More Research-Intensive and Integrated European Research Area. *Science, Technology and Competitiveness Key Figures Report*, *2009*. Retrieved December, 2020 from http://aei.pitt.edu/46028/1/Key_figures_2008.pdf

Fighter aircraft in Encyclopedia Britannica: https://www.britannica.com/technology/military-aircraft

G. M. Levchuk, Y. N. Levchuk, Jie Luo, K. R. Pattipati and D. L. Kleinman, "Normative design of organizations. I. Mission planning," in IEEE Transactions on Systems, Man, and Cybernetics - Part A: Systems and Humans, vol. 32, no. 3, pp. 346-359, May 2002, doi: 10.1109/TSMCA.2002.802819.

Haico te Kulve, H., & Smit, W. A. (2010). Novel naval technologies: Sustaining or disrupting naval doctrine. Technological forecasting and social change, 77(7), 999-1013.

Harris, Charles E., James H. Starnes Jr, and Mark J. Shuart. "Design and manufacturing of aerospace composite structures, state-of-the-art assessment." Journal of aircraft 39.4 (2002): 545-560.

Hartley, K., & Belin, J. (Eds.). (2019). *The Economics of the Global Defence Industry*. Routledge.

Horgan, J., & Toal, D. (2006, December). Review of machine vision applications in unmanned underwater vehicles. In 2006 9th International Conference on Control, Automation, Robotics and Vision (pp. 1-6). IEEE.

https://nso.nato.int/natoterm/content/nato/pages/ntp.html?lg=en

https://www.fieldtechnologiesonline.com/doc/wireless-glossary-of-terms-0001

INTERNATIONAL JOURNAL OF INFORMATION SECURITY SCIENCE M. Karamanetal., Vol.5, No.1. Institutional Cybersecurity from Military Perspective

Introduction to the special issue on secure communications. Telecommun System 69, 169 (2018). https://doi.org/10.1007/s11235-018-0455-z

J. Alves et al., "Vehicle and Mission Control of the DELFIM Autonomous Surface Craft," 2006 14th Mediterranean Conference on Control and Automation, Ancona, 2006, pp. 1-6, doi: 10.1109/MED.2006.328689.

J. Cortes, S. Martinez, T. Karatas and F. Bullo, "Coverage control for mobile sensing networks," in IEEE Transactions on Robotics and Automation, vol. 20, no. 2, pp. 243-255, April 2004, doi: 10.1109/TRA.2004.824698.

J. García, D. Gonzalez, A. Rodríguez, B. Santamaria, J. Estremera and M. Armendia, "Application of Impedance Control in Robotic Manipulators for Spacecraft On-orbit Servicing," 2019 24th IEEE International Conference on Emerging Technologies and Factory Automation (ETFA), Zaragoza, Spain, 2019, pp. 836-842, doi: 10.1109/ETFA.2019.8869069.

Kok, Joost N., et al. "Artificial intelligence: definition, trends, techniques, and cases." Artificial intelligence 1 (2009).

Laudon, K. C., & Laudon, J. P. (2011). Essentials of management information systems. Upper Saddle River: Pearson.

Manseur, R. (1997, November). Development of an undergraduate robotics course. In Proceedings Frontiers in Education 1997 27th Annual Conference. Teaching and Learning in an Era of Change (Vol. 2, pp. 610-612). IEEE.

Manufacturing In Britannica: https://www.britannica.com/technology/manufacturing

Medlin, R. C. (2001). U.S. Patent No. 6,327,954. Washington, DC: U.S. Patent and Trademark Office.

Michael Pinedo, Scheduling Theory, Algorithms, and Systems,Prentice Hall, 2002, p 1

Missile In Merriam-Webster's dictionary: https://www.merriam-webster.com/dictionary/missile

Morin, Pascal, and Claude Samson. "Trajectory tracking for non-holonomic vehicles: overview and case study." Proceedings of the Fourth International Workshop on Robot Motion and Control (IEEE Cat. No. 04EX891). IEEE, 2004.

Munkres, James. "Algorithms for the assignment and transportation problems." Journal of the society for industrial and applied mathematics 5.1 (1957): 32-38.

Nagahdaripour, S., Xu, X., & Khamene, A. (1998, September). Applications of direct 3D motion estimation for underwater machine vision systems. In IEEE Oceanic Engineering Society. OCEANS'98. Conference Proceedings (Cat. No. 98CH36259) (Vol. 1, pp. 51-55). IEEE.

Public Safety Canada. 2010. Canada's Cyber Security Strategy. Ottawa: Public Safety Canada, Government of Canada.

Razani, M. (2018). Commercial Space Technologies and Applications: Communication, Remote Sensing, GPS, and Meteorological Satellites. CRC Press.

Reconnaissance In Merriam-Webster's dictionary: https://www.merriam-webster.com/dictionary/reconnaissance

Robinson, Robert F., and John E. Counts. "Methods for Analyzing the Contributions of C 3 and C 3 CM to Military Force Capabilities." Systems Analysis and Modeling in Defense. Springer, Boston, MA, 1984. 237-249.

Satellites In Merriam-Webster's dictionary: https://www.merriam-webster.com/dictionary/satellites

Schedule In Merriam-Webster's dictionary: https://www.merriam-webster.com/dictionary/schedule

Schutt, Rachel; O'Neil, Cathy (2013). Doing Data Science. O'Reilly Media. ISBN 978-1-449-35865-5.

SIPRI (2019), *The SIPRI Top 100 arms-producing and military services companies in the world (excluding China).* SIPRI Arms Industry Database [database]. Retrieved June, 2020 from https://www.sipri.org/databases/armsindustry

Smith, M. B. (2014, April). Disruptive naval technologies. In NDIA 15th Annual Science and Engineering Technology Conference.

Space technology In Wikipedia https://en.wikipedia.org/wiki/Space_technology

Stover, J. A., & Gibson, R. E. (1992, July). Modeling confusion for autonomous systems. In Science of Artificial Neural Networks (Vol. 1710, pp. 547-555). International Society for Optics and Photonics.

Swyter, H. (1970). Political considerations and analysis of military requirements for chemical and biological weapons. Proceedings of the National Academy of Sciences of the United States of America, 65(1), 261

Tarantilis C. (2008) Routing Vehicles, Algorithms. In: Shekhar S., Xiong H. (eds) Encyclopedia of GIS. Springer, Boston, MA

Tetley, L., & Calcutt, D. (2007). Electronic navigation systems. Routledge.

The Future of Sea Power. Proceedings of the RAN Sea Power Conference 2015. Edited by Andrew Forbes

United Nations Development Programme. Evaluation Office. (2002). Handbook on monitoring and evaluating for results. Evaluation Office.

Veruggio, G., & Operto, F. (2006). Roboethics: a bottom-up interdisciplinary discourse in the field of applied ethics in robotics. International review of information ethics, 6(12), 2-8.

White, F. E. (1991). Data fusion lexicon. Joint Directors of Labs Washington DC.

Xia, B. S., & Gong, P. (2015). Review of business intelligence through data analysis. Benchmarking, 21(2), 300-311. doi:10.1108/BIJ-08-2012-0050