R1.2 ANNEX 1 - Data driven analysis for the Defence Technology Roadmap

Dissemination level: PU (public)

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

Index

1. Introduction 4
2. Industrial needs 4
2. Results from data-driven analysis 5
2.1 Robotics, AI & autonomous-system 6
2.1.1 Applications of robotics, AI & autonomous-system domain 6
2.1.2 Classify and rate technologies: robotics, AI & autonomous-system domain 10
2.1.3 Relevance matrix: robotics, AI & autonomous-system domain 13
2.2 C4ISTAR 14
2.2.1 Applications of C4ISTAR domain 15
2.2.2 Classify and rate technologies: C4ISTAR domain 17
2.2.3 Relevance matrix: C4ISTAR domain 21
2.3 Cybersecurity 22
2.3.1 Applications of Cybersecurity domain 23
2.3.2 Classify and rate technologies: Cybersecurity domain 24
2.2.3 Relevance matrix: Cybersecurity domain 27
3. Conclusion 29
Appendix 1. AAU & PRZ Industrial Survey 32
Appendix 2. Technologies description – AAU and PRZ team 1
Appendix 3. Results of the technologies classification – AAU and PRZ team 10
Appendix 4. Results of the relevance matrix– AAU and PRZ team 11
Appendix 5. Results of the applications identification – UNIPI and UNIBX team 13
Appendix 6. Results of the technologies identification – UNIPI and UNIBX team 14
Appendix 7. Results of the relevance matrix – UNIPI and UNIBX team 23
Appendix 8. UC3M & UNISEVILLE Industrial Survey 25
Appendix 9. Technologies description – UC3M and UNISEVILLE team 31
Appendix 10. Results of the relevance matrix– UC3M and UNISEVILLE team 33
References 34

Figure index

Figure 1- Relevance matrix of robotics, AI & autonomous-system domain..... 14
Figure 2 - Research Activity and Development Activity graphs..... 18
Figure 3 - Relevance matrix of the C4ISTAR domain. 22
Figure 4 - Relevance matrix of the cybersecurity domain. 28
Figure 5 - Evolution of number of papers referencing the technologies. 10
Figure 6 - First version of Relevance matrix. 11
Figure 7 - Relevance matrix of the robotics, AI & autonomous-system domain. 12
Figure 8 - Heatmap of Relevance matrix. 23
Figure 9 - Network of technologies and applications in C4ISTAR domain. 24
Figure 10 - Relevance matrix of the cybersecurity domain. 33

Table index

Table 1 - List of macro applications with relevant examples for AI, Robotics and Autonomous Systems..... 9
Table 2 - List of operative applications and relationship to macro applications..... 10
Table 3 - Classification of robotics, AI & autonomous-system technologies. 13
Table 4 - Description of quantitative scores for the classification of the technologies. 18
Table 5 - Classification of C4ISTAR technologies. 21
Table 6 - Classification of cybersecurity technologies. 27
Table 7 - Table of overlaps among technologies and application within the domains. 29
Table 8 - List of technologies from expert knowledge. 9
Table 9 - The technologies identified in the Cybersecurity domain. 32

1. Introduction

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

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

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

This document contains: a description of the industrial needs within the defence sector, and the analysis on the technologies within the three domains. The technology analysis consists of:

1. **Identifying, scoring and categorising relevant technologies –** this was achieved in the following manners:
    a. **Automatically** by extracting keywords from academic and defence-oriented databases such as Scopus and STO. This is the approach adopted by the C4ISTAR team.
    b. Using **expert knowledge** which is the approach followed by the Cybersecurity team.
    c. Using both **automated approach and expert knowledge** from academia and industry (through surveys). This is the approach adopted by the robotics, AI and autonomous systems team.
2. **Identifying potential application domains –** this consists in finding relevant defence applications where technologies can be a game changer.
3. **Mapping the technologies to applications –** this consists in estimating the relevance of a given technology for a specific application domain using scores.

2. Industrial needs

The industrial needs can be derived from the challenges that the defence industry is facing:

- the reduction of public investment;
- the faster technology development;
- the increase of technological complexity.

Since the end of the Cold War, European countries has reduced the amount of public expenditure in defence, leading companies to adapt to the new economic context and to find financial sources in order to maintain and improve their competitive position. This has for consequence the need of flexibility for the companies and an evolution from pure firms (firms operating only in defence) to dual firms (firms operating both in defence and civil).

The evolution of technologies in various domains related to the defence is even faster and more complex than in the past, especially due to the disruptive technologies, and thus for all the technological domains in

ASSETs+ (e.g. the technological complexity brought by implementation of information and communication technologies in weapon systems).

With regards to **robotics, AI and autonomous-systems**, various technologies and skills are needed to have a strong defence industry. Based on the feedback from Leonardo and Saab, such profiles include specialists in Artificial intelligence (AI), robotics, autonomy, additive manufacturing, data sciences, high performance computing (HPC), simulation, internet of things (IoT), edge computing, information and communication technologies, autonomous-systems and systems engineering processes. The feedbacks from these companies are the results of an industrial survey, that is reported in the Appendix 1 "*AAU & PRZ Industrial Survey*".

Such profiles are needed in high-priority defence applications such as space technologies, cyber security and resilience, missile manufacturing, autonomous-system design, fighter aircraft engineering, sensor systems and planning, command and control systems. According to the industrial partners of ASSETs+ project, this significant gap between the defence sector and education is mainly due to bad recognition, importance and impact of defence sector on society.

For the **C4ISTAR** domain the challenges doubles down because technologies in this domain are many and very different from each other due to the great range of goals indicated by the acronym itself: Command, Control, Communication, Computer, Intelligence, Surveillance, Target Acquisition, and Reconnaissance. Moreover, the use of technologies related to C4ISTAR is already massive in civil applications. Traditionally defence research brings development in civil. Now it is the opposite. This changes in the path of R&D lead defence firms to adapt to these technological changes as well as to a transformation in innovation practices [1]. In this regard, partnerships, collaboration and knowledge sharing, also at an international level, are a crucial element to face the lack of specific capabilities and keep the pace of innovation.

The defence industrial base (DIB) is expected to show competence in **cybersecurity** to, at least, support adequate protection of sensitive information (see NIST 800.171 for a list of requisites for US DoS contractors [2]). Furthermore, it would be highly desirable that the hardware and software products produced by defence industry comply with the strict security standards described in regulation and/or good practices. It must be noted that Europe itself counts on a substantial technological dependence, as it has already been pointed out by the European Parliament's scientific foresight unit [3]. Thus, adequate (re)training in cybersecurity is among the essential industrial needs in the EU, as a means to achieve a stronger European ICT industry.

2. Results from data-driven analysis

This paragraph presents the results of technology road mapping in the three different domains:

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

Each of the following sections describes the outcomes within a specific domain. There are three key concepts at stake for this document – skills, applications and technologies. They are intimately linked each other, since users with *skills* exploit *technologies* for specific defense-related *applications*.

The technology roadmap describes the evolution of the core technologies in the domains and their applications related to defence area, providing the actual picture and the path for monitoring changes over the time. It includes:

1. The identification of the relevant application in the given domain;
2. The identification and the classification of the technologies in the given domain;
3. The identification of the relationships among the applications and technologies, described in Relevance matrix.

2.1 Robotics, AI & autonomous-system

An autonomous-system is a device or a software 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. [17]

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. [18, 19]

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. [20]

2.1.1 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). [21]
- **Anomaly detection:** refers to the problem of finding patterns in data that do not conform to expected behavior. [22]
- **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. [23, 24]
- **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. [25, 26]
- **Combat simulation**: Representations of military operations using gaming and calculation, with or without man-in-the-loop for training, analysis, and research. [27]
- **Cyber resilience:** the ability to continuously deliver the intended outcome despite adverse cyber events [28]

- **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. [29, 30]
- **Fighter aircrafts**: military vehicle (plane) provide control over the necessary airspace by driving away or destroying an enemy aircraft. [31] 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. [32] 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. [33, 34] 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. [35] 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. [36]
- **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. [37]
- **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. [21] 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. [38, 39, 40]
- **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. [41]
- **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. [43]

- **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. [44, 45]

- **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. [46, 47]

- **Space technologies:** technology developed by space science or the aerospace industry for use in spaceflight, satellites, or space exploration [48]. 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. [49]

- **Surveillance**: The systematic observation of aerospace, cyberspace, surface, or subsurface areas, places, persons, or things by visual, aural, electronic, photographic, or other means. [43]

- **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. [50]

- **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. [51]

- **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). [52, 53, 54]

- **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. [55, 56, 57]

- **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. [58] Important issues here are weapon designing, weapon manufacturing, weapon testing, weapon reliability.

Note that the above list contains both macro and micro (operative) applications. Table 1 shows the list of macro applications with some examples and operative applications (from but not not restricted to Table 2) for the three technology fields.

Macro application	AI	Robotics	Autonomous systems
Aeronautics	Anomaly detection	Manufacturing	Autonomous Mobile Robots (AMR) Autonomous Intelligent Vehicles (AIV) Unmanned Aerial Systems (UAS)
Combat simulation	Simulated aerial combat	Military Training Robots	Vehicle and agent simulation
Cyber resilience	Prediction and detections of adverse events Reinforcement learning	Robotic platforms	Autonomous mobility systems
Cyber security	Automatic detection of anomalies	Robotic platforms	Autonomous mobility systems
Fighter aircrafts		Aircraft manufacturing	
Land armours	Model optimisation	Armour manufacturing	
Military vehicle manufacturing	Anomaly detection	Component manufacturing	Routing
Missile	Target tracking	Manufacturing	Trajectory tracking
Mission control	Plan updating and adjustment	Path planning	
Mission planning	Vehicle routing		Scheduling
Naval	USV routing Combat Management System	USV manufacturing	Trajectory tracking Autonomous Unmanned Surface Vehicles (USV)
Reconnaissance	Guiding patrolling missions	A robotic system for reconnaissance	Autonomous, urban reconnaissance robot
Rescue	Intelligent Systems for Search and Rescue	Assignment	Area coverage optimisation
Underwater	Anomaly detection	Submarine manufacturing	Trajectory tracking Unmanned Undersea Vehicles (UUV)
Satellites	Automate image	Component manufacturing	Coverage
Space technologies	Anomaly detection	Space robots	Coverage
Surveillance	Assignment	Tactical Surveillance Robots	Coverage
Weapons	Autonomous weapons systems (AWS)	Manufacturing	Autonomous weapons systems (AWS)

Table 1 - List of macro applications with relevant examples for AI, Robotics and Autonomous Systems.

On the second hand, the Table 2 shows the identified operative applications and the macro applications they belong to/are relevant for.

Operative application	Macro applications mainly relevant for
Anomaly detection	Aeronautics, cyber security, mission planning and control, naval, space technologies, surveillance, underwater, satellites, weapons
Assignment	Aeronautics, mission planning and control, rescue, satellites
Coverage	Mission planning and control, rescue, surveillance, satellites
Path planning	Aeronautics, mission planning and control, naval, rescue, underwater
Routing	Aeronautics, mission planning and control, naval, rescue, underwater

Scheduling	Aeronautics, military vehicle manufacturing, mission planning and control, rescue, satellites
Target tracking	Missile, mission planning and control, satellites
Trajectory tracking	Missile, mission planning and control, satellites

Table 2 - List of operative applications and relationship to macro applications.

It is worth noting that each of the identified operative applications are relevant for multiple high-level applications. As macro applications can cover all the operative applications, we will consider option 2 (remove operative applications).

2.1.2 Classify and rate technologies: robotics, AI & autonomous-system domain

The Table 1 contains the list of robotics, AI & autonomous-system technologies identified in the defence sector with both qualitative and quantitative measures. The descriptions of these technologies are reported in the Appendix 2. The quantitative scores used to rate technologies in this domain are:

- **Score 1** represents the number of papers referencing the keyword between 2009 and 2019.
- **Score 2** represents the research productivity:

$$Score\ 2 = log(Score\ 1) / max\_papers(2019:2009) * 10$$

- **Score 3** represents the research trend:

$$Score\ 3 = 100 * sum\_papers(2019:2015) / sum\_papers(2019:2009)$$

- **Score 4** is the research variability:

$$Score\ 4 = stdev(sum\_papers(2019:2009)) / avg\_papers(2019:2009)$$

- **Score 5** is a measure representing the recency of the technology:

$$Score\ 5 = (sum\_papers(2020) * 4 + sum\_papers(2019)) / 2\ ) / avg\_papers(2015:2019)$$

- **Score 6**: since the interest is particularly directed to the technologies that are well-studied (score 1), trending (score 3), and novel (score 5), this score combines these 3 properties using the following weighted-sum formula. The score 1 is prioritized to the others to ensure that all the extracted keywords are well investigated by the research community:

$$score\ 6 = (3/5) * (score\ 1 / max(score\ 1)) + (2/5) * (score\ 3 / max(score\ 3) + score\ 5 / max(score\ 5))$$

Using score 6, the list containing 109 keywords is sorted and the top 37 keywords are selected. Furthermore, the list is extended with 3 keywords identified based on the partner input: Human Machine Interaction; High performance computing; Structures and Materials.

Note that a qualitative approach based on expert judgement is used to determine the level of maturity and abstraction. Therefore, we used three levels of abstraction: high (abstract or general concepts), medium (higher level of specificity and specialisation) and low (specific technologies). On the other hand, the levels of maturity are more focused on applicability and can be determined as: Established (technologies widely studied and tested in academia and adopted within industry), Mature (technologies investigated and tested in academia and somehow adopted within industry) and Emerging (new technologies investigated in academia with less adoption within industry).

Technology	Maturity	Abstraction	Score 1	Score 2	Score 3	Score 4	Score 5	Score 6
Artificial Intelligence	**Mature**	**High**	3170475	0.0002	51.781	9889.645	0.730	0.430
Autonomous-system	**Established**	**High**	15857	0.0204	52.217	52.438	0.775	0.173
Robotics	**Established**	**High**	973274	0.0005	53.568	4640.829	0.738	0.252
Simulation	**Mature**	**Medium**	7223484	0.0001	50.656	18745.285	0.742	0.766
Optimization	**Established**	**Medium**	5356097	0.0001	55.114	31691.580	0.829	0.627
Sensor	**Mature**	**Medium**	2704485	0.0002	54.084	13733.434	0.777	0.400
Explainable artificial intelligence	**Emerging**	**High**	1451	0.0517	96.278	426.291	2.176	0.381
Blockchain	**Emerging**	**Low**	32188	0.0034	99.540	8437.375	1.811	0.359
Deep learning	**Mature**	**Medium**	300600	0.0005	96.336	57124.749	1.485	0.347
Reasoning network	**Emerging**	**Medium**	327	0.2647	72.171	25.869	2.320	0.345
Edge computing	**Mature**	**Medium**	27934	0.0040	98.196	6552.136	1.633	0.340
Signal processing	**Mature**	**Medium**	2062191	0.0002	52.251	7187.808	0.704	0.337
Image Semantic Segmentation	**Emerging**	**Low**	686	0.1187	92.128	124.628	1.737	0.335
Machine learning	**Mature**	**Medium**	1322399	0.0002	65.230	30242.400	0.988	0.326
Fog computing	**Emerging**	**Low**	20861	0.0057	98.317	4098.075	1.391	0.319
Neural network	**Mature**	**Low**	1163585	0.0003	62.448	21284.828	1.017	0.310
Big data	**Mature**	**Medium**	440894	0.0005	89.688	44307.358	1.047	0.307

Technology	Maturity	Abstraction	Score 1	Score 2	Score 3	Score 4	Score 5	Score 6
Adversarial machine learning	**Emerging**	**Low**	1887	0.0454	94.330	376.906	1.341	0.305
Clustering	**Mature**	**Medium**	1378292	0.0003	55.065	7931.699	0.805	0.295
Internet of Things	**Emerging**	**Medium**	284914	0.0007	86.595	27001.547	1.035	0.287
Soft robotics	**Emerging**	**Medium**	13594	0.0112	85.707	1262.149	1.211	0.278
3D printers	**Emerging**	**Low**	61272	0.0031	88.367	5570.383	0.976	0.267
5G	**Emerging**	**Low**	145567	0.0013	86.317	13167.212	0.925	0.265
Cyber physical system	**Established**	**Medium**	14750	0.0099	91.342	1787.437	0.902	0.263
Computer vision	**Mature**	**Medium**	906886	0.0004	56.805	7528.038	0.797	0.258
Reinforcement learning	**Emerging**	**Medium**	142861	0.0018	64.213	3602.874	1.104	0.236
Support vector machine	**Mature**	**Low**	318418	0.0011	61.702	4759.770	0.933	0.231
Cloud computing	**Established**	**Medium**	324138	0.0010	67.683	9208.280	0.763	0.229
Autonomous vehicle	**Mature**	**Medium**	30983	0.0068	68.550	1074.927	1.000	0.227
Natural language processing	**Mature**	**Low**	213968	0.0015	61.001	2856.792	0.824	0.211
Augmented reality	**Emerging**	**Medium**	112134	0.0025	64.926	2473.468	0.821	0.211
GPS	**Established**	**Low**	418017	0.0011	52.930	1796.748	0.710	0.202
Fuzzy logic	**Mature**	**Medium**	318186	0.0013	53.417	1319.098	0.791	0.202

Technology	Maturity	Abstraction	Score 1	Score 2	Score 3	Score 4	Score 5	Score 6
Voice recognition	**Mature**	**Low**	9716	0.0253	60.570	126.653	0.901	0.200
Human Machine Interaction	**Mature**	**Medium**	7518	0.0333	58.460	83.616	0.773	0.185
High performance computing	**Mature**	**Medium**	169151	0.0024	55.067	1141.438	0.630	0.179
Structures and Materials	**Mature**	**Medium**	39940	0.0073	62.669	632.397	1.060	0.221
Additive manufacturing	**Mature**	**Medium**	Included based on survey					
Automation	**Mature**	**High**	Included based on survey					

Table 3 - Classification of robotics, AI & autonomous-system technologies.

A visualization of the evolution of the number of papers published by the selected technologies, reported in the Table 3, is presented in Appendix 3.

2.1.3 Relevance matrix: robotics, AI & autonomous-system domain

The Relevance matrix of Robotics, AI & autonomous-system applications and technologies is generated based on the number of papers containing both the technology and the application for each pair of technology-application. Afterwards, the results are normalized in the interval [0,10] using logarithmic scale as described in the document R1.1 “Strategy Specification”.

The relevance matrix, shown in figure 1, identified many potential technologies that can be used for specific defence applications. In particular, AI, simulation, optimization, sensors, autonomous-systems and robotics span a various number of applications where they can be utilized. A different visualization of this result is reported in Appendix 4. Based on the investigation there are many technologies that are highly relevant to the defence sector. In particular, simulation, optimisation, big data, machine learning and high-performance computing.

	Mission planning	Mission control	Reconnaissance	Surveillance	Routing	Scheduling	Assignment	Coverage	Rescue	Target tracking	Combat simulation	Military vehicle manufacturing	Missile guidance	Anomaly detection	Trajectory tracking	Path planning	Space technologies	Cyber security	Cyber resilience	Aeronautics	land armours	Naval	Underwater	Satellite	Weapons	Fighter aircrafts
Artificial Intelligence	8	8	7	7	6	6	7	7	6	7	7	6	6	6	5	7	8	7	5	5	0	7	6	6	7	4
Autonomous system	8	9	8	8	6	6	7	7	6	8	8	6	6	5	6	7	8	6	5	6	0	7	7	7	7	4
Robotics	7	7	6	7	5	5	5	6	5	6	6	5	5	4	5	6	7	5	3	4	0	6	6	6	6	3
Simulation	9	10	8	9	7	7	8	8	7	8	10	7	7	6	7	8	9	7	6	7	0	9	7	8	9	5
Optimization	8	9	8	8	7	7	7	8	6	8	8	7	6	6	6	7	8	6	5	7	0	8	6	7	8	5
Sensor	9	9	8	9	7	7	7	8	7	9	8	7	7	7	7	8	9	7	5	7	0	8	7	8	8	5
Explainable artificial intelligence	4	4	3	4	1	1	3	3	2	3	3	2	1	1	0	3	4	4	3	0	0	3	2	2	3	0
Blockchain	1	1	0	2	1	0	0	1	0	2	0	0	0	1	1	0	2	2	0	0	0	0	0	1	1	0
Deep learning	7	7	6	7	5	5	6	6	5	6	7	5	6	5	5	6	7	6	5	5	0	6	5	6	7	4
Reasoning network	7	8	7	7	6	6	7	7	6	7	7	5	6	5	5	7	7	6	4	5	0	7	5	6	7	4
Edge computing	7	7	6	7	6	5	6	6	5	6	7	6	5	5	5	6	7	6	4	6	0	6	5	6	6	4
Signal processing	8	8	8	9	6	6	7	8	6	8	8	6	6	6	7	7	8	6	4	6	0	8	7	8	8	5
Image Semantic Segmentation	3	3	3	3	3	2	3	3	3	3	3	3	3	2	1	3	3	2	1	2	0	3	2	3	3	1
Machine learning	8	8	7	7	6	6	6	7	6	7	7	6	6	5	6	7	8	6	5	5	0	7	6	6	7	4
Fog computing	5	5	5	5	4	4	4	5	4	5	5	4	5	3	4	5	5	3	1	4	0	5	4	4	5	3
Neural network	7	7	6	7	5	6	6	6	5	6	7	5	5	5	5	6	7	5	4	5	0	6	5	6	6	4
Big data	8	8	7	8	6	6	7	7	6	7	7	6	6	6	6	7	8	7	5	6	0	7	6	7	7	5
Adversarial machine learning	5	5	4	5	3	4	4	4	3	4	4	4	4	4	3	4	5	4	4	3	0	4	3	4	5	2
Clustering	6	6	5	6	5	5	5	6	4	6	6	4	4	4	4	5	6	5	3	4	0	6	4	5	5	3
Internet of Things	7	7	6	7	6	6	6	6	5	6	7	5	6	5	5	6	7	6	5	5	0	7	5	6	7	4
Soft robotics	5	5	5	5	4	4	4	5	4	5	5	4	4	3	3	5	5	4	2	4	0	5	4	5	5	1
3D printers	3	3	3	3	3	2	2	3	3	3	3	3	3	1	2	3	3	1	0	2	0	3	2	3	3	0
5G	4	5	4	4	3	3	2	3	3	4	4	3	3	2	3	4	5	2	1	3	0	3	3	4	4	1
Cyber physical system	7	7	5	6	5	5	5	6	5	6	6	4	5	4	4	6	7	7	6	4	0	6	4	5	6	2
Computer vision	8	8	7	7	6	6	7	7	6	7	8	6	6	5	6	7	8	6	5	6	0	7	6	7	7	4
Reinforcement learning	6	6	5	5	4	4	5	5	4	5	5	4	4	3	4	5	6	5	3	4	0	5	4	5	6	2
Support vector machine	6	7	6	7	5	5	6	6	5	6	6	5	5	5	5	6	7	5	4	5	0	6	5	6	6	4
Cloud computing	6	7	6	6	5	5	5	6	5	6	6	5	5	4	5	6	7	6	4	5	0	6	4	6	6	3
Autonomous vehicle	8	8	7	8	6	6	6	7	6	7	7	6	6	5	6	7	8	6	5	6	0	7	7	7	7	4
Natural language processing	7	7	6	7	6	6	6	7	6	7	7	6	6	5	5	7	7	6	5	5	0	7	5	6	7	4
Augmented reality	7	7	6	7	5	6	6	6	6	7	7	5	6	4	5	6	7	5	4	5	0	7	5	6	7	4
GPS	7	8	7	8	6	5	6	7	6	7	7	5	6	5	6	7	7	5	3	5	0	6	6	7	7	4
Fuzzy logic	6	6	5	6	4	5	5	5	4	5	6	4	5	4	4	5	6	4	3	4	0	5	4	5	6	3
Voice recognition	7	7	6	6	5	5	6	6	5	6	6	5	5	4	4	6	7	5	3	4	0	6	4	5	6	4
Human Machine Interaction	8	8	7	7	6	6	7	7	6	7	8	6	6	5	6	7	8	6	5	5	0	7	6	6	7	4
High performance computing	8	8	7	8	6	6	7	7	6	7	8	6	6	6	6	7	8	7	5	6	0	7	6	7	7	4
Structures and Materials	7	8	7	7	5	6	6	7	6	7	8	7	6	5	5	6	8	5	4	6	1	7	5	7	7	5
Additive manufacturing	0	0	0	0	0	0	0	0	0	0	0	7	0	0	0	0	7	0	0	7	6	7	7	7	6	6
Automatoin	9	9	7	7	9	9	9	9	7	9	6	9	9	9	8	9	6	7	5	6	5	6	6	8	6	5

Figure 1- Relevance matrix of robotics, AI & autonomous-system domain.

It is important to keep in mind that an association between two keywords does not necessarily imply the relevance of the technology for the defence application. Therefore, the relevance matrix is revised by experts to determine which pair of technology-applications are relevant in the defence sector, in the specific case of robotics, AI & autonomous-system domain. The version of the relevance matrix obtained by expert judgment is reported in Appendix 4.

2.2 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.

2.2.1 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. [59]
- **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. [59, 60]
- **Communication**: Communication is the transfer of intelligence, knowledge or information according to agreed conventions. [61]
- **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. [60]
- **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. [62]
- **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. [59]
- **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. [63]
- **Decision Making**: Decision Making is the process of choosing among several alternative possibilities. [64]
- **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. [65]

- **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. [59]
- **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. [59]
- **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. [66]
- **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. [59]
- **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. [67]
- **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. [68]
- **Programming**: Programming is the process of translating the system specifications prepared during the design stage into program code. [69]
- **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. [59]
- **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. [70]
- **Surveillance**: Surveillance is the systematic observation of aerospace, surface, subsurface areas, places, persons, or things by visual, electronic, photographic, or other means. [59]
- **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. [59]

The complete list of the identified applications in the C4ISTAR domain is reported in Appendix 5.

2.2.2 Classify and rate technologies: C4ISTAR domain

The classification of technologies related to the C4ISTAR domain, presented in this paragraph, is based on the maturity level and the abstraction level. The evaluation of the maturity level is enhanced by quantitative scores related to scientific publications and patents. Table 4 describes the scores and the rating methods. To have a clear overview of scientific and technical knowledge production, different time intervals are chosen, i.e. from 2002 to 2019 for papers and from 2000 to 2017 for patents, both related to the C4ISTAR domain. The difference is due to the timing in the patenting process. More specifically, when a patent is filed in a patent office, it requires an examination to be granted before its publishing, and this period usually lasts 18 months.

Score	Description	Meaning
$Recent\ Research\ Ratio = \frac{\sum_{t=2015}^{2019} x}{\sum_{t=2002}^{2019} x} \times 100$ where x = number of papers in a year t = time interval	Total number of papers in the last 5 years of the given period divided by the total number of papers in the whole period, expressed as a percentage.	It measures the research interest in a given technology, considering the amount of ideas generated in the last years compared to the overall period.
$Recent\ Development\ Ratio = \frac{\sum_{t=2013}^{2017} x}{\sum_{t=2000}^{2017} x} \times 100$ where x = number of patents in a year t = time interval	Total number of patents in the last 5 years of the given period related to the total number of patents in the whole period, as percentage.	It measures the industrial interest in a given technology, considering the amount of technical developments in the last years compared to the overall period.
$Research\ Growth\ Index = \frac{\bar{x}\,[t1]}{\bar{x}\,[t2]}$ where $\bar{x}$ = mean of the number of papers in a given time interval $t1$ = time interval from 2018 to 2019 $t2$ = time interval from 2013 to 2017	The mean of papers in the last 5 years of the given period divided by the mean of papers in the previous 5 years.	It measures the growth in production of new scientific knowledge. The more the value is greater than 1, the more the technology is being developed in recent years compared to the past.
$Development\ Growth\ Index = \frac{\bar{x}\,[t1]}{\bar{x}\,[t2]}$ where $\bar{x}$ = mean of the number of patents in a given time interval	The mean of patents in the last 5 years of the given period related to the mean of patents in the previous 5 years.	It measures the growth in production of new technical knowledge. The more the value is greater than 1, the more the technology is being developed in

Score	Description	Meaning
$t1$ = time interval from 2016 to 2017 $t2$ = time interval from 2011 to 2015		recent years compared to the past.

Table 4 - Description of quantitative scores for the classification of the technologies.

The indicators Recent Research Ratio, Research Growth Index and Recent Development Ratio, Development Growth Index are used to respectively measure respectively Research Activity and Development Activity, as shown in Figure 2, where, for better visualization, only some of the technologies are labelled.

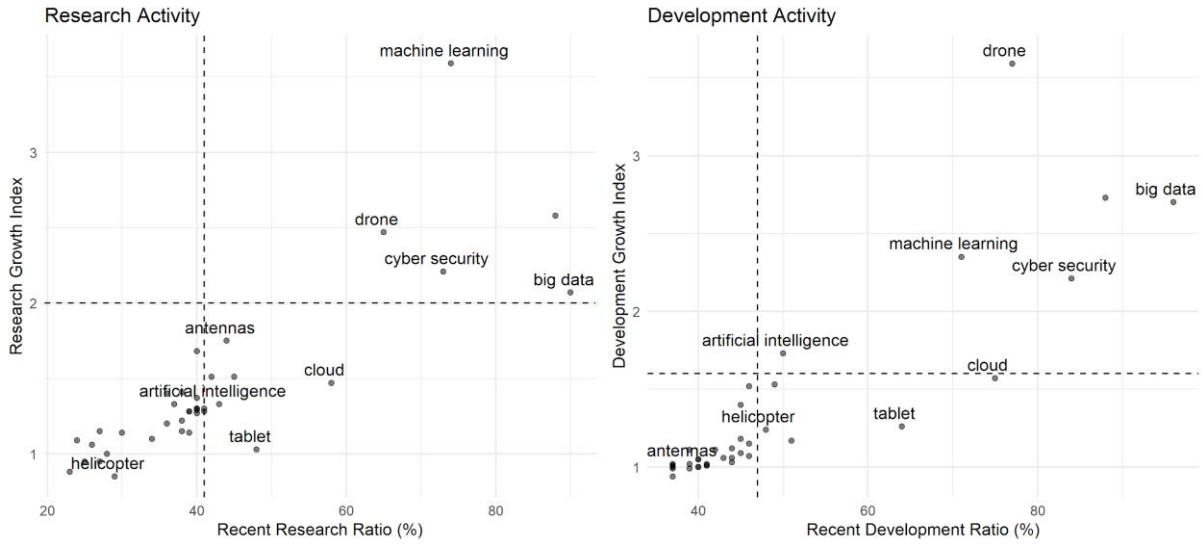


Figure 2 - Research Activity and Development Activity graphs.

Therefore, a classification of maturity level is defined based on the position of each point among the 4 parts of the two graphs in Figure 2.

The evaluation of the abstraction level is based on expert judgment. The Table 5 shows the list of identified technologies related to the C4ISTAR domain, with their maturity level, as well as the quantitative scores used to define it, and their abstraction level.

Technology	Maturity	Abstraction	Recent Research Ratio (%)	Recent Development Ratio (%)	Research Growth Index	Development Growth Index
Big data	**Emerging**	**Low**	90	96	2.07	2.7
Cybersecurity	**Emerging**	**High**	73	84	2.21	2.21
Data analytics	**Emerging**	**High**	88	88	2.58	2.73
Drone	**Emerging**	**Low**	65	77	2.47	3.59

Technology	Maturity	Abstraction	Recent Research Ratio (%)	Recent Development Ratio (%)	Research Growth Index	Development Growth Index
Machine learning	**Emerging**	**Low**	74	71	3.59	2.35
Artificial intelligence	**Mature**	**High**	43	50	1.33	1.73
Antennas	**Established**	**Low**	44	39	1.75	1.02
Cameras	**Established**	**Medium**	41	46	1.3	1.15
Cloud	**Established**	**Low**	58	75	1.47	1.57
Console	**Established**	**Low**	30	51	1.14	1.17
Helicopter	**Established**	**Medium**	29	48	0.85	1.24
Intelligence system	**Established**	**High**	42	49	1.51	1.53
Receivers	**Established**	**Low**	41	37	1.28	0.99
Tablet	**Established**	**Low**	48	64	1.03	1.26
Vehicles	**Established**	**Medium**	45	39	1.51	1.11
Aerial	**Outdated**	**High**	40	37	1.3	1.01
Communications systems	**Outdated**	**High**	36	41	1.4	1.02
Ethernet	**Outdated**	**Medium**	25	45	0.95	1.09
Gateways	**Outdated**	**Medium**	38	44	1.41	1.12

Technology	Maturity	Abstraction	Recent Research Ratio (%)	Recent Development Ratio (%)	Research Growth Index	Development Growth Index
Information system	**Outdated**	**High**	27	37	0.95	0.94
Interfaces	**Outdated**	**Low**	34	39	1.1	0.99
Internet	**Outdated**	**High**	40	41	1.68	1.01
Linux	**Outdated**	**Medium**	28	46	1	1.07
Management system	**Outdated**	**High**	39	40	1.28	1
Mobile	**Outdated**	**Low**	40	41	1.3	1.01
Operating systems	**Outdated**	**High**	39	43	1.14	1.06
Radar	**Outdated**	**Medium**	39	46	1.28	1.52
Radio	**Outdated**	**High**	36	40	1.2	1.05
Robot	**Outdated**	**High**	40	45	1.37	1.4
Router	**Outdated**	**Low**	23	45	0.88	1.18
Satellites	**Outdated**	**Medium**	40	40	1.29	1.05
Sensor	**Outdated**	**Medium**	40	42	1.27	1.11
Server	**Outdated**	**Low**	37	44	1.33	1.06
Software	**Outdated**	**High**	38	40	1.22	1

Technology	Maturity	Abstraction	Recent Research Ratio (%)	Recent Development Ratio (%)	Research Growth Index	Development Growth Index
Surveillance systems	**Outdated**	**High**	38	37	1.15	1
User interface	**Outdated**	**Low**	24	44	1.09	1.03
Workstations	**Outdated**	**Low**	27	37	1.15	1.02

Table 5 - Classification of C4ISTAR technologies.

The technologies reported in Table 3 are the 37 most relevant for the C4ISTAR domain and represent a part of the large list of 2030 technologies extracted with the methodology presented in the document R1.1 “Strategy Specification”. The complete list of technologies is reported in Appendix 6.

2.2.3 Relevance matrix: C4ISTAR domain

The Relevance matrix of the C4ISTAR applications and technologies is generated based on the number of papers, extracted with a specific query for the C4ISTAR domain. Afterwards, the results are normalized in the interval [0,10] using logarithmic scale as described in the document R1.1 “Strategy Specification”. The Relevance matrix is reported in Figure 3. Moreover, other visualizations are provided in Appendix 7.

	communication	simulation	monitoring	programming	planning	identification	data processing	decision making	navigation	positioning	information exchange	mission	surveillance	data analysis	logistic	imagery	authentication	encryption	remote control	data fusion	command and control	messaging	reconnaissance	target acquisition	military intelligence
intelligence system	5	4	4	4	4	4	4	5	3	3	3	3	4	4	3	2	2	2	2	3	3	2	3	0	2
console	6	5	5	5	4	4	5	4	4	4	4	4	4	4	3	3	3	3	4	2	3	3	3	1	0
cyber security	6	5	5	5	5	5	4	5	4	3	5	4	4	4	3	2	5	5	3	3	4	3	3	1	1
linux	6	6	6	6	4	5	5	4	4	4	5	4	4	5	3	3	5	4	4	3	3	4	2	0	0
data analytics	6	5	6	5	5	5	6	6	4	4	4	4	4	6	5	3	4	4	2	4	2	3	2	0	1
ethernet	7	6	6	6	5	4	5	4	4	4	6	4	4	4	3	3	4	4	5	3	3	4	2	1	0
router	8	7	6	6	5	5	5	5	4	5	6	4	4	4	3	2	5	5	4	4	3	4	2	0	1
tablet	7	6	7	5	6	6	5	5	5	5	4	4	5	5	5	4	5	4	4	3	2	4	2	2	0
gateways	7	7	6	6	5	5	5	5	4	5	6	5	4	4	5	3	5	5	4	4	3	4	3	0	1
helicopter	6	7	6	5	6	6	5	5	6	5	4	6	5	4	5	5	2	2	4	4	4	2	5	3	2
workstations	7	7	6	7	6	5	6	5	5	5	6	5	4	5	4	4	4	4	4	3	4	4	3	2	0
surveillance systems	6	6	7	5	6	6	6	5	5	4	4	4	8	5	6	4	4	4	4	4	3	3	4	2	1
operating systems	7	7	7	8	6	6	6	5	6	5	6	5	5	5	4	4	5	5	5	4	4	5	3	1	1
big data	7	7	7	6	6	6	7	7	5	5	6	5	6	7	6	5	5	6	3	5	3	4	3	1	2
drone	7	7	7	6	7	6	5	6	7	6	5	7	6	4	5	6	4	4	5	5	5	3	6	4	2
antennas	9	9	7	6	6	7	6	5	7	7	6	7	6	5	5	6	4	4	5	5	4	3	5	3	1
machine learning	7	7	7	7	7	7	7	7	6	6	5	5	6	7	7	6	5	5	4	5	4	4	4	2	1
management system	8	8	7	7	7	7	7	7	6	6	6	6	6	6	6	5	6	5	5	5	5	5	4	2	0
server	8	8	7	7	6	7	7	6	6	6	7	5	6	6	5	5	7	7	6	5	5	6	4	1	1
user interface	8	8	7	8	7	6	7	7	7	6	6	6	5	6	5	5	6	5	6	5	5	5	4	4	1
cameras	7	8	8	7	7	7	7	6	7	7	5	7	7	6	5	7	5	5	6	6	4	4	6	4	1
radar	8	8	8	6	7	7	7	6	7	7	5	7	7	6	5	8	4	4	5	6	5	3	6	5	2
cloud	8	8	8	7	7	7	7	7	6	6	6	7	6	7	6	7	7	7	5	5	4	5	4	3	1
receivers	9	9	8	7	6	7	7	7	7	8	7	6	6	6	8	6	6	6	5	5	4	4	4	3	1
robot	8	9	7	8	8	7	6	7	8	7	6	7	6	5	6	5	5	4	7	6	5	4	5	4	2
artificial intelligence	8	8	7	8	8	7	7	8	6	6	6	6	6	7	6	6	6	6	5	6	5	5	4	3	3
radio	9	9	8	7	7	8	7	6	8	7	7	7	6	6	6	5	6	6	6	6	5	5	5	3	2
communications systems	10	9	8	7	7	7	7	7	7	7	9	7	6	6	6	5	6	6	6	5	5	6	5	3	2
satellites	9	8	8	7	7	7	7	7	8	8	6	8	7	7	6	8	5	5	5	6	5	4	6	4	3
internet	9	8	8	8	8	8	8	8	7	7	8	6	7	7	7	6	7	7	6	5	5	6	4	2	2
information system	9	8	8	8	8	8	8	8	7	7	7	7	7	7	7	7	6	6	5	6	5	6	5	3	3
vehicles	8	9	8	8	8	8	7	7	8	8	7	8	7	6	7	7	6	5	6	6	6	5	6	5	2
aerial	8	9	8	8	8	8	7	7	8	8	6	8	7	7	7	8	5	5	6	6	6	4	7	5	3
interfaces	9	9	8	9	8	8	8	8	7	7	7	7	6	7	6	7	6	6	7	6	6	6	5	4	2
mobile	10	9	8	8	8	8	8	8	8	8	8	7	7	7	7	6	7	7	6	6	5	7	5	4	2
sensor	9	9	9	8	8	8	8	7	8	8	7	8	8	7	6	8	7	6	7	8	6	5	6	5	3
software	9	10	9	9	9	8	8	8	8	7	8	7	7	8	7	7	7	7	6	6	6	6	5	4	3

Figure 3 - Relevance matrix of the C4ISTAR domain.

The relevance matrix registers the highest score for the combination of the following technologies: internet, information system, vehicles, aerial, interfaces, mobile, sensor, software; and applications: communication, simulation, monitoring, programming, planning, identification. Therefore, those are the first topics to address in designing the educational programmes.

2.3 Cybersecurity

Cybersecurity involves a great deal of techniques for the protection of systems, devices and networks, against damage to availability, integrity, authentication, confidentiality, and non-repudiation. 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). Although the aforementioned goals stand across a wide range of scenarios and applications, the techniques and protection measures in place should be fit for the needs of each particular case. As such, our objective is to find technologies and applications used in cybersecurity for the purpose of attacking or defending in defence-related scenarios. Indeed, the Joint Research Centre (JRC), the European Commission's science and knowledge service, already pointed out the defense sector as part of the cybersecurity taxonomy [95]. Moreover, the Council of the European Union developed the EU Cyber Defence Policy Framework [95], highlighting the need of building a strong force in the EU to respond to cyberattacks. It must be noted that while attacking is not the goal of ASSETS, knowledge about their related technologies is paramount for a proper defense strategy. It must be noted that selecting the most relevant technologies that should be at stake in future training/skilling/upskilling initiatives is relevant to achieve the notion of Digital Strategic Autonomy, defined by the European Cybersecurity Agency (ENISA) as "the ability of Europe to source products and services designed to meet the EU's specific needs and values, while avoiding being subject to the influence of the outside world" [96]. The set of skills needed to exploit (or related to) the set of technologies identified herein will be subject of later analysis in the next deliverable R.1.3.

Methodological note

Cybersecurity issues in the defence sector are commonly considered as sensitive information. As such, public records may be more scarce than in other domains which suggest that our methodology needs to complement a data-driven approach with expert judgement more heavily than in the remaining technological domains (e.g., robotics/AI and C4ISTAR). Nevertheless, a positive aspect is that cybersecurity counts on several public documents issued by well-known reputed organizations such as the American's NIST which provide an excellent baseline for the identification and classification of technologies related to cybersecurity. Another particularity of our methodology is the consideration of sources of information from four different views or perspectives: (a) industrial perspective; (b) regulation and good practices perspective; (c) academia and research perspective; and (d) military and defence perspective. We have put more emphasis in the content found in (a), (b) and (d) and less in (c).

Considering the above, the work carried out in the cybersecurity field is based on existing documents, which are systematically analyzed by USEV and UC3M expert judgment. The relevance of each technology per application has been determined by USEV and UC3M sub teams in the first version. To avoid any sub team-related bias, both USEV and UC3M proposed a rating independently and discussions were held in case of discrepancies. Moreover, they will be confronted with external experts from industry and academia in the annual revisions following ASSETS+ planning.

2.3.1 Applications of Cybersecurity domain

The identified potential defence applications related to the cybersecurity domain are 8 and the list has been generated by selecting applications based on their occurrence in a set of domain documents. For this, we used a data-driven approach followed by manual inspection of the results as explained in the document R1.1 "Strategy Specification". 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. [7]

- **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. [71]
- **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). [72]
- **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. [73] This has already been pointed out as a future key research direction by ENISA [97].
- **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. [72]

2.3.2 Classify and rate technologies: Cybersecurity domain

The classification of technologies related to the cybersecurity domain is based on the maturity level and the abstraction level, which are rated as follows:

- **Maturity level** is classified based on the results of an industrial survey and a data driven approach that takes into account the data provided from ECSO and the number of the scientific papers related to the cybersecurity domain (collected from Scopus).
- **Abstraction level** is measured based on the expert judgement, also considering the nature of the technologies reported in ECSO market radar.

The metrics analyzed in the industrial survey are:

- **Perceived maturity** is the maturity level of a given technology perceived by the industrial area. Each company evaluates a given technology on three levels that are low, medium and high. However, for the sake of analysis, it has been converted into a quantitative dimension by computing the mean among all answers, considering low maturity as 1, medium as 2 and high as 3.
- **Relevance** refers to the relevance of the technologies within the defence area for each of surveyed companies. As in the previous case, it is converted into a quantitative dimension following the same procedure.

The survey addressed to companies to measure the relevance of each technology in the defence sector is reported in the Appendix 8.

The Maturity Level combines the perceived maturity within companies and the relevance in the defence sector. Thus, the values are given as follows:

- Relevance ≤ 1.6: *Outdated*
- Perceived maturity and relevance is in [1.6, 2.0]: *Emerging*
- Perceived maturity and relevance is in (2.0, 2.4]: *Mature*
- Perceived maturity and relevance is in (2.4, 3.0]: *Established*

A Scopus search query is defined for each technology to extract all the related scientific papers. This research allows to clarify the scope of the technology, reduce overlapping, and investigate specific properties of the technology, in particular level of maturity or research interest. The quantitative scores used in the bibliometric analysis are:

- **Number of EU companies** with expertise in the technology. This is based on the ECSO market radar, complemented with ad-hoc searches;
- **Overall Papers (OP)**: number of papers (after 2009) matching the query;
- **Research trend (RT)**: the ratio of OP published between 2015 and 2019;
- **Research variability (RV)**: the coefficient of variation of the number of papers over the last 11 years. Low values imply that the research is quite stable (the topic is still alive);
- **Recent Research Index (RR)** number of papers in the years 2020 and 2019 divided by number of papers in the previous 4 years.

The Table 6 contains the list of cybersecurity technologies related to the defence area with both qualitative and quantitative measures. The descriptions of these technologies are reported in the Appendix 9.

Technology	Maturity	Abstraction	Perceived Maturity	Relevance	EU comp.	OP	RT	RV	RR
Identification & Authentication	**Mature**	**Low**	2.4	2.4	8	2008	34	3	10
Authorization & Access Control	**Mature**	**Low**	2.4	2.4	8	24397	30	11	7
Firewalls	**Established**	**Low**	2.6	2.4	8	4655	29	6	10
Cyber range	**Mature**	**Low**	2.4	2.2	9	80	91	12	37
Encryption	**Established**	**Low**	2.6	2.6	10	35443	49	325	13
Certification	**Established**	**Low**	2.8	2.4	5	410	30	1	13

Technology	Maturity	Abstraction	Perceived Maturity	Relevance	EU comp.	OP	RT	RV	RR
Endpoint Security	**Mature**	**Low**	2.2	2	9	3524	57	68	11
Mobile & IoT Security	**Mature**	**Low**	2.2	2.4	12	14176	66	1602	5
Cloud and virtualization security	**Outdated**	**Low**	2	1.6	8	4760	56	71	7
Vulnerability management	**Mature**	**Medium**	2	2.4	15	296	60	8	11
Malware analysis	**Mature**	**Low**	2.6	1.8	5	807	60	15	9
Hardware security	**Established**	**Low**	2.8	2.2	12	4056	80	250	9
Intrusion Prevention/Detection Systems (IDS/IPS)	**Mature**	**Low**	2.2	2.2	14	14085	31	35	11
Cyber threat Intelligence	**Mature**	**Medium**	1.8	2.4	17	100	97	20	23
Honeypots	**Outdated**	**Low**	1.6	1.4	6	653	44	4	12
Security Operations	**Emerging**	**Medium**	1.8	2.2	14	1397	43	5	8
Risk assessment & management	**Mature**	**High**	2.2	2.4	10	242	67	11	17
Compliance and assurance	**Established**	**High**	2.6	2.4	13	154	69	7	12
Secure software development	**Established**	**High**	2.6	2.4	9	393	48	4	13
Forensic analysis	**Mature**	**Low**	2.2	2	14	119	50	3	14
DoS Protection	**Mature**	**Low**	2.2	2	6	1774	44	16	17
Cyber resilience	**Established**	**Medium**	2.4	2.4	9	2513	42	15	9

Technology	Maturity	Abstraction	Perceived Maturity	Relevance	EU comp.	OP	RT	RV	RR
Open Source Intelligence (OSINT)/ Private Intelligence (PRIVINT)	**Emerging**	**Low**	1.8	2.2	1	134	51	3	21
Penetration Testing / Red Teaming	**Emerging**	**Low**	2	1.8	4	446	55	6	11

Table 6 - Classification of cybersecurity technologies.

The quantitative scores from the bibliometric analysis are not directly used to define maturity level and abstraction level. Those are measured in order to in order to inspire the design of courses. In fact, they will prioritise which technologies are relevant and for future iteration of this task, they can be used for comparison.

Based on these findings, several issues can be noticed. On the one hand, there is no direct connection between what companies perceive as mature or relevant and the research efforts carried out in scientific papers. For example, compliance and assurance technologies, and encryption ones offer very similar indicators of maturity and relevance, but their research profile is substantially different.

There is also a lack of connection between maturity and the amount of companies offering a given technology. For instance, cyber threat intelligence is offered by 17 companies while OSINT/PRIVINT ones are only carried out by 1, while both of them are similar in terms of maturity and relevance.

Despite these misalignments, it must be noted that some connections arise, especially in the extreme cases. Thus, those technologies which count on the biggest amount of papers (encryption, authorization and identification, mobile security and IDS/IPS) are regarded as highly mature and relevant by industrial stakeholders.

2.2.3 Relevance matrix: Cybersecurity domain

The Relevance matrix of the Cybersecurity applications and technologies is generated based on expert judgment. Two sub-teams (one from the U3CM and another one from UNISEVILLE) have assessed the relevance independently and results have been discussed until a final agreement was reached. The CV of the members of both sub-teams are provided in R.1.1. The results are shown in Figure 6 by using the relevance score and a colour scale: from 0, meaning no relevant, to 10, meaning high relevant. A different visualization of this result is reported in Appendix 10. In the future, we would like to enhance our matrix with other data-driven approaches or with a survey.

	Defense industrial base collaboration	Cyber security awareness and training	Operations Security (OPSEC)	Cyber Operations (CO)	Military Information Support Operations (MISO)	Command and Control Support	Secure Communications (COMSEC)	Cyber electronic warfare activities (CEWA)
Identification & Authentication	7	2	7	7	7	8	8	7
Authorization & Access Control	9	3	10	9	9	9	10	8
Firewalls	10	3	9	9	1	3	9	8
Cyber range	0	10	9	9	1	3	0	8
Encryption	9	1	9	8	6	6	10	7
Certification	9	1	8	3	2	3	9	7
Endpoint Security	10	1	9	8	3	3	7	7
Mobile & IoT Security	3	3	7	8	2	2	0	3
Cloud and virtualization security	3	2	7	6	3	3	0	2
Vulnerability management	10	1	9	9	2	2	0	6
Malware analysis	7	3	7	7	0	0	0	3
Hardware security	9	3	9	3	3	3	0	10
Intrusion Prevention/ Detection Systems (IDS/IPS)	9	2	9	8	3	2	8	8
Cyber threat Intelligence	9	6	6	7	7	7	0	10
Honeypots	0	0	7	7	0	0	0	3
Security Operations	9	3	10	7	6	8	7	7
Risk assessment & management	10	3	9	8	2	2	0	8
Compliance and assurance	10	3	7	2	3	3	9	7
Secure software development	8	1	7	2	2	2	0	9
Forensic analysis	8	3	3	9	1	1	0	3
DoS Protection	9	3	9	7	3	3	10	10
Cyber resilience	7	3	9	7	10	10	6	10
Open Source Intelligence (OSINT)/ Private Intelligence (PRIVINT)	7	8	6	10	8	8	0	3
Penetration Testing / Red Teaming	9	10	3	10	3	3	0	10

Figure 4 - Relevance matrix of the cybersecurity domain.

Results show that the most relevant technologies considering those that are applied in 5 or more applications are: Identification & Authentication, Authorization & Access Control, Firewall, Encryption, Endpoint Security, Intrusion Prevention/Detection Systems (IDS/IPS), Security Operations, DoS Protection, Cyber resilience.

3. Conclusion

The Table 5 shows the technologies, in blue, and the applications, in orange, included in more than one domain. Moreover, it presents also the numbers of observations that have no overlaps.

	Robotics, AI and autonomous systems	C4ISTAR	Cybersecurity
Mission planning and control			
Reconnaissance			
Surveillance			
Target Acquisition And Tracking			
Aerial/Aeronautics			
Satellite			
Cyber security awareness and training			
Cyber resilience			
Simulation			
Cloud computing and virtualization security			
Big data			
Machine learning			
Robotics			
Sensor			
Surveillance systems			
Mobile & IoT Security			
Authentication, Authorization & Access Control			
Encryption			
Identification & Authentication			
Number of other Applications	20	20	7
Number of other Technologies	35	33	22

Table 7 - Table of overlaps among technologies and application within the domains.

Several entries are classified as technologies in one area and as application in another one. This evidence is correct under a conceptual perspective, furthermore, it brings out bridges between the various domains. Those linkages could be a starting point for the design of the educational and training programmes to produce a greater impact within the scope of our project.

The following evidences can be derived from the Table 5:

1. there is a strong overlap between the robotics, AI and autonomous systems domain and the C4ISTAR domain, both for the technologies and the applications;
2. there is an overlap between the C4ISTAR domain e the cybersecurity domain;
3. there is a weak overlap between the robotics, AI and autonomous systems domain and the cybersecurity domain, limited to the security aspects;
4. cloud computing and virtualization security is the only common technology within the three domains.

Another important evidence is that “artificial intelligence”, “cybersecurity” and “command and control” come out as technologies or application in the domains. Since they are also the fields themselves, this

outcome allows to identify the main relationships among them. In general, the C4ISTAR domain appears as a strong connecting element with the two other fields. This is due both to the C4ISTAR technologies and to the application-based features of those technologies. This situation can be summarised in the Figure 5. In particular, the robotics, AI and autonomous systems domain is related to the C4ISTAR domain for all the topics and to the cybersecurity domain for what concern AI technologies, as indicated with the different colours in the Figure 5.

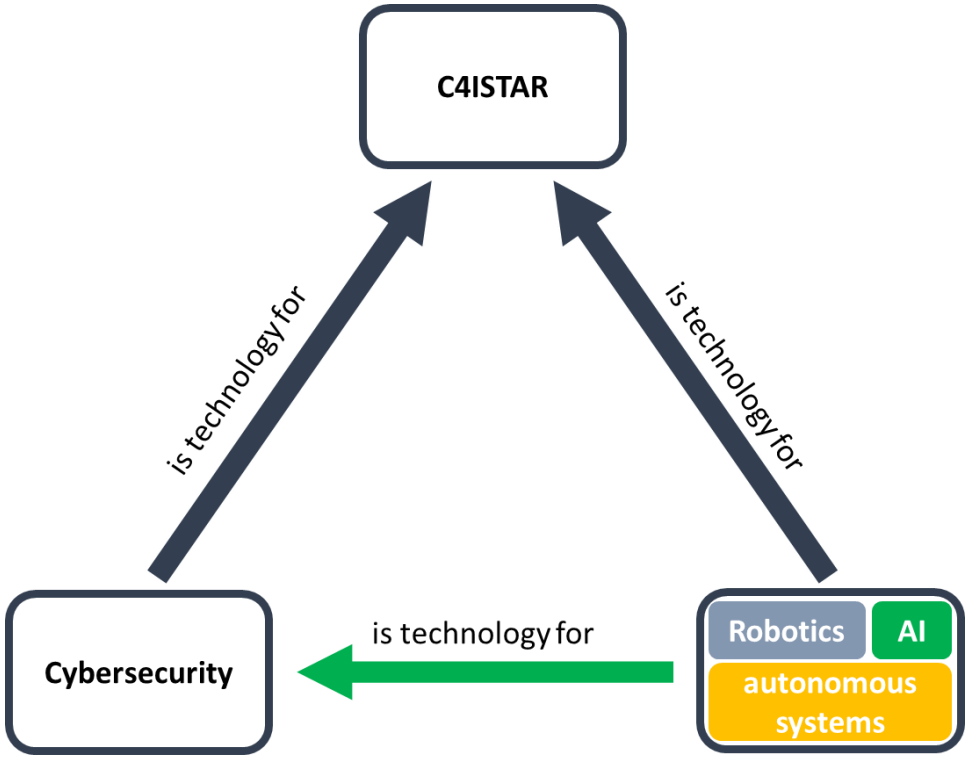


Figure 5 - Connection among the domains.

The C4ISTAR domain includes systems, tools and devices that create Situational Awareness and support decision making, information sharing and data fusion, promoting interoperability and integration during actions. For this reason, C4ISTAR enhances Robotics, AI and autonomous systems domain and needs Cybersecurity to operate properly in the Defence sector. Given its characteristics C4ISTAR is the bonding agent of the domains in ASSETs+.

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 onw 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.

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

Appendix 1. AAU & PRZ Industrial Survey

This appendix contains the industial survey conducted by AAU and PRZ team.

QUESTIONNAIRE

Skills & Technology mapping

in

AI & robotics, Cybersecurity and C4ISTAR

Date:

- 16/03/2020: 1st draft;

Authors: Aalborg University
Revised:
Validated:
Approved:

Industrial partners

Q. What technologies do your company specialise in?

A.

- Sensor systems and functions
- Command, Control, Communication, Cyber
- Software Intensive Systems and Information and Communication Technologies
- Human Machine Interaction and Autonomous Systems
- Vehicle Sub-Systems
- Engineering Methods and Tools
- Vehicle Engineering
- Production Systems and Manufacturing
- Structures and Materials
- Maintenance and Logistics Support
- Training and simulations
- Weapons Technology

Q. What defence applications and subfields do your company specialised in?

A.

- Aeronautics
- Advanced weapons systems
- Command and control systems
- Sensors
- Underwater systems

Q. What future skills and personnel profiles are required in your company to improve your products and services?

A.

Future skills:

- Artificial intelligence and Machine Learning
- Additive Manufacturing
- Automation
- Cyber security
- Digitalisation and Information Technologies
- Modelling and simulation

Personnel profiles:

- Knowledge sharing and collaborative technical leaders with organisational dexterity and with a passion for learning and innovation.

Q. Do your company already have these necessary skills?

A. Yes, but we still need to broaden and deepen our skills

Q. Which skill gaps cause the most concern in your company?

A. The new skills and jobs that does not yet exist

Q. What causes these skill gaps?

A. Due to technology advancement and demographic change in combination of our long product life cycles

Q. What technologies are lacking to improve your company product or services?

A. We are not missing anything but we need to accelerate the change

Q. Do you see a different need for technology specialists or technology/product generalists in the future?

A. No

Q. What current opportunities do your employees have for learning and gaining future skills?

A. We use the 70:20:10-model mind-set.

70 % - On the job training and challenging assignments. We also use innovation labs where employees work in projects (teams) with entrepreneurial or intrapreneurial activities

20 % - coaching and mentoring in different forms

10 % - formal training (class room and online learning)

Q. What aspects do you think create a gap between the current defence-oriented educational programmes and new technologies?

A.

- Autonomy
- Hypersonic Speed
- Propulsion technologies
- Additive manufacturing
- Robust communication
- Defensive cyber

Q. What defence applications/subfields should be prioritised?

- Missiles
- Underwater systems
- Autonomous vehicles
- Fighter aircrafts
- Sensor systems
- Command and control systems

Educational institution Partners

Q. What technologies are taught at your institute and how are they relevant for defence?

A.

Q. What EQF levels is the institute teaching?

A.

Q. What are the formats of the courses taught at the institute?

A.

Q. What pre-skills/experiences do students need?

A.

Q. Are your current teachers ready to accommodate the special learning needs of post-secondary students?

A.

Q. What aspects do you think create a gap between the current defence-oriented educational programmes and new technologies?

A.

Q. What defence applications/subfields should be prioritised?

A.

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

QUESTIONNAIRE

Skills & Technology mapping

in

AI & robotics, Cybersecurity and C4ISTAR

Date:

- 16/03/2020: 1st draft;

Authors: Aalborg University
Revised:
Validated:
Approved:

Industrial partners

Q. What technologies do your company specialize in?

A.

Q. What defence applications and subfields do your company specialised in?

A.

Q. What future skills and personnel profiles are required in your company to improve your products and services?

A.

Q. Do your company already have these necessary skills?

A.

Q. Which skill gaps cause the most concern in your company?

A.

Q. What causes these skill gaps?

A.

Q. What technologies are lacking to improve your company product or services?

A.

Q. Do you see a different need for technology specialists or technology/product generalists in the future?

A.

Q. What current opportunities do your employees have for learning and gaining future skills?

A.

Q. What aspects do you think create a gap between the current defence-oriented educational programmes and new technologies?

A.

Q. What defence applications/subfields should be prioritised?

A.

Educational institution Partners

Q. What technologies are taught at your institute and how are they relevant for defence?

A.

Mercantec – Centre for Advanced Technology teaches a variety of different technical education which includes different competences and technologies.
2011 Mercantec was appointed "Centre of Excellence" by the Confederation of Danish Industry"
2018 Mercantec became member of "National Center for automation and robotics"

Competences and technologies are not necessarily linked to a single education or program but converges among different educations – therefore the following list of technologies are picked from different educational programs and contexts.

- *Manufacturing – we teach manufacturing (SM) using milling machines and lathes up to 5 axis and we just installed a milling tool using a robot. This technology where we combine robotics and milling is quite unique and has been part of our "National Knowledge enter for automations and Robotics". In connection with manufacturing we teach materials science so that the students experience the different possibilities and limitations and correct choice of tools and technics according to material.*
- *AM is taught as an integrated subject within the SM – combining and comparing the different manufacturing methods. We are teaching 3D printing in different polymer materials combined with Kevlar and carbon*
- *Advanced welding technics – using different welding methods and materials – automated welding using robots*
- *Automechanics – we teach all aspects of repair and maintenance of vehicles and motors (diesel, gasoline, hybrid and hydrogen (we are one of the first VET schools in EU to teach hydrogen vehicles)) – primarily cars.*
- *Engineering and system integration – at our automation and robotics centre we teach a great variety of different technologies:*
  - Programming of PLC's (Siemens, Allen Bradley, Omron, Schneider)
  - working with hydraulic and pneumatic systems
  - handling and programming of Robots (KUKA, Fanuc, ABB) and Cobots (UR5)
  - setting up and troubleshooting on complex and fully automated conveyor systems
  - we also teach system integration under the umbrella of Industry 4.0
- *Cyber security – this is taught at our data department who educates IT-supporters and data technicians/engineers. In the field of data handling we furthermore teach,*
  - basic and advanced programming using the most popular languages among others #C, python, C++, SWIFT
  - AI and machine learning
  - industrial use of data – how is data collection and handling activated in an industrial environment
  - data centres – we have developed a special education program aiming at staff working at data centres
- *Drones – at our electronics department we work with drones – especially from a configuration and maintenance perspective.*

Q. What EQF levels is the institute teaching?

A.

EQF levels 4 and 5

Q. What are the formats of the courses taught at the institute?

A.

Courses may vary in length and format from 1 day to 2-3 weeks. The courses are mainly facilitated as ordinary presence courses, but can be tailormade to customers wishes including partial or total online courses. (some limitations due to using equipment)

Q. What pre-skills/experiences do students need?

A.

Depending on EQF level. Some courses are taught at high levels and will require basic pre-skills other courses are taught af lower or basic levels and will require no pre-skills other than basic understandings

Q. Are your current teachers ready to accommodate the special learning needs of post-secondary students?

A.

Yes – the relevant teachers are already involved in further training and education teaching also at post-secondary levels. The involved teacher will typically hold a candidates or bachelor's degree or have a substantially experience form working life

Q. What aspects do you think create a gap between the current defence-oriented educational programmes and new technologies?

A.

The new technologies are emerging at the speed of lightning which means that 1) we are not able to teach and train at the same speed – this creates a gab between what is technological possible and practical possible. This also means that companies will have severe difficulties in utilising and commercialise the new technologies because of lack of skills.

So actually developing the right skills to link between R&D and production is one of the main issues this is what we do!

Q. What defence applications/subfields should be prioritised?

A.

Our only actual engagement defence related is teaching and training NATO crew in digital infrastructures including security.
So from that point of view we are convinced that cyber security must be prioritised - along with robotics and system integration / engineering.

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

QUESTIONNAIRE

Skills & Technology mapping

in

AI & robotics, Cybersecurity and C4ISTAR

Date:

- 16/03/2020: 1st draft;

Authors: Aalborg University
Revised:
Validated:
Approved:

Industrial partners

Q. What technologies do your company specialize in?

A. Defence and security electronics, Sensors, Electronic warfare, Cybersecurity, big data, robotics

Q. What defence applications and subfields do your company specialised in?

A. **Mission Management Systems**: HENSOLDT designs Maritime Surveillance (SURMAR) and Intelligence, Surveillance, and Reconnaissance (ISR) systems to equip aircraft used for air-ground or air-sea reconnaissance. Furthermore, HENSOLDT has developed an embedded Combat Management System (CMS) for surveillance and coastal defence.

Radar, IFF, Data Link: HENSOLDT's Radar, IFF & Datalink portfolio covers mission-critical premium products in the area of military and security radar, air traffic control/identification-friend-or-foe (IFF) and datalinks for air, sea, and land platforms to various platform manufacturers worldwide.

Optronics: Our optronics portfolio covers optronic, optic and precision-engineered products for military, civil and security applications. HENSOLDT deploys optronics solutions on various platforms, including submarines, armoured vehicles, aircraft, unmanned aerial vehicles and satellites

Spectrum Dominance and Airborne solutions: a comprehensive portfolio for Electronic Warfare and Signal Intelligence, which is evolving towards also supporting Cyber Operations. Our Airborne Solutions range from Avionics components and systems to complex Integrated Airborne Mission Systems, as well as Unmanned Solutions.

Q. What future skills and personnel profiles are required in your company to improve your products and services?

A. Following profiles are required for our future product development,

System Architect:

- Model Based System Engineering (MBSE)
- Knowledge of multi-sensor architecture
- Knowledge of network architecture, communication systems
- Knowledge of ARP4754 / ARP4761 and MIL STD
- Knowledge in the area of requirements engineering
- General understanding of wide variety of engineering disciplines (systems, software, hardware, EMC, RF, V&V, safety, security)
- Knowledge of embedded or real-time system development
- General understanding of aircraft avionics or naval systems (Control Systems, Navigation Systems, Communications, Stores Management)

Software Architect:

- Software modelling (UML)
- Distributed software architectures
- Network architectures

- Data distribution systems
- Data storage systems
- Software scheduling
- Security and safety considerations
- Hypervisor, micro-kernel, containers
- Standard protocols/buses (IP, MILSTD-1553, CAN)
- Knowledge of DO-178 standard
- Knowledge of embedded or real-time software development

Data Processing Developer:

- Data Fusion
- Data Classification/Identification
- Target Tracking
- Artificial Intelligence applied to Sensor Processing
- Machine Learning algorithms
- Big Data Processing and Data Analytics
- Bulk Data Processing Techniques
- High Performance Computing (HPC), GPU programming
- Data Visualisation
- Image and video processing

Sensor design expert (Radar, IFF or ASuW sensor):

- Signal processing
- Sensor Array processing
- General Experience in Radar System Design
- Knowledge of RADAR (AESA/PESA/MSA) and active/passive radars
- Professional experience in the fields of IFF and system design of IFF systems
- Knowledge and experience in design and qualification of ASuW architectures (Antisurface Warfare)
- Knowledge of ASuW sensors (active and passive) and ASuW weapon systems
- Knowledge of all cross-sectional aspects for ASuW sensors

Security Engineer:

- Understanding of architecture, administration, and management of operating systems and networking systems.
- Cryptography, network security, access management and defensive coding practices
- Programming/software development concepts and software analytics skills
- Threat modelling, specifications, implementation, testing, and vulnerability assessment
- Knowledge of Cyber security standards/regulations

FPGA Developer:

- Experience in FPGA development and integration (e.g. for avionics equipment)
- ASIC (application-specific integrated circuit) knowledge (e.g. for avionics equipment)
- Design and implementation of signal/image processing algorithms, AI algorithms and high-speed interface
- Knowledge of international HW development standards
- Knowledge of RTCA/DO-254 standard

Database/Data Mining Developer:

- MDB (Multi-Dimensional Database)
- OLAP (Online Analytical Processing)
- Cloud computing
- Mass storage architecture

Data Visualization Engineer:

- Data visualisation technics (multi-source, multi-dimensional data, scalar/vectors/text/image/video, 2D/3D/4D, charts, maps)
- Visual ergonomics (information distribution)
- Geographical Information System (GIS)
- Massive Data exploration, filtering, searching
- Timeline/time series representation & navigation
- Data animation

Network/Communication Engineer:

- Data Link (Air, Ground or UAV)
- SATCOM network
- Wireless communication/networks
- Routers, gateways, firewalls

Electronic Warfare Expert:

- Electronic protection (EP)
- Electronic warfare support (ES) & Signals intelligence (SIGINT) : Spectrum Dominance, Communications Warfare, Communications Intelligence

General Personal skills:

- self-organisation, self-reflection, resilience
- Intercultural cooperation
- Ability to motivate teams
- Strong communication skills
- Innovative and self-motivated attitude
- Analytical and conceptual skills
- Creativity
- Ability to solve complex problems
- Entrepreneurial thinking
- Leadership skills
- Ability to assess performance, time and cost estimates
- Customer orientation

Q. Do your company already have these necessary skills?

A. Here, the combination of skills is the most problematic, coupled with the corresponding professional experience. Many candidates can do a bit of everything, but we do not need them that urgently. We need those candidates who have a particularly good knowledge of certain areas. In general, we find it very

difficult to find e.g. system engineers or software developers/software architects who have, at best, relevant experience in our products/our industry.

Q. Which skill gaps cause the most concern in your company?

A. Our company has a continuous watch on following critical skills:

1. Skills related to our specific product area (C4ISTAR system, radar sensors…) e.g. Profiles like Sensor design expert, Electronic Warfare Expert
2. Skills related to new technologies or emerging areas (R&D areas): e.g. like Data Mining Developer or Data Processing Developer, Data Visualization Engineer

Q. What causes these skills gaps?

A.

1. The first cause of skill shortage is due to a small-size population of candidates for our C4ISTAR and sensors development needs. Competitors quickly catch these “experts” and they have a very low job mobility.
2. Candidates with new technologies skills are massively employed by company from civil areas (financial field, manufacturing, industry…)

Q. What technologies are lacking to improve your company product or services?

A.

Technologies in the field of machine learning, e.g. deep learning, random forests, CRFs, SVMs, etc.

Technologies for high performance data processing or for image/video processing, e.g. Open CV, Open CL, Cuda, MatLab, Tensor Flow

Q. Do you see a different need for technology specialists or technology/product generalists in the future?

A. For successful achievement of our product development, we need mixed teams with specialists and generalists. Team skills should be complementary:

- Some product generalists with global overview of system capabilities and architecture

- Some specialists to refine and implement specific needs.

Note: Beyond the mix of skills, lack of female engineers is also a big issue. Companies, universities, schools and governments/EU should deal this problem of gender balance.

Q. What current opportunities do your employees have for learning and gaining future skills?

A. Mostly classical presence training and e-learning

Q. What aspects do you think create a gap between the current defence-oriented educational programmes and new technologies?

A. New technologies are emergent technologies with, sometimes, low maturity level. These areas are limited to a small-sized pool of experts. It is probably difficult to match an educational program with industrial experience, due to a lack of feedback about technology usage, and the confidentiality of defence-related subjects. Lecturers can only write program from public sources, like research papers or open source projects.

Q. What defence applications/subfields should be prioritised?

A. Relevant applications/subfields:

- Electronic warfare

- Data security & system resiliency (data integrity, communication & service continuity)

- Multi-source data analysis

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

QUESTIONNAIRE

Skills & Technology mapping

in

AI & robotics, Cybersecurity and C4ISTAR

Filled: LEONARDO SPA 08-04-2020
Date:

- 16/03/2020: 1st draft;

Authors: Aalborg University
Revised:
Validated:
Approved:

Industrial partners

Q. What technologies do your company specialize in?

A. materials, electronics, software, mechanics, systems engineering, optronics,

Q. What defence applications and subfields do your company specialised in?

A. aeronautical, land armours, naval, underwater, cyber, communications, satellite, robotics

Q. What future skills and personnel profiles are required in your company to improve your products and services?

A. Systems Engineering Processes, Information and Communication Technologies, Cybersecurity, Interoperability, Software Engineering, Artificial Intelligence (ML/DL), Big Data Analytics, IoT / Edge Computing, High Performance Computing, Robotics / Unmanned Autonomous Systems

Q. Do your company already have these necessary skills?

A. partially

Q. Which skill gaps cause the most concern in your company?

A. artificial intelligence, cyber security, robotics

Q. What causes these skill gaps?

A. internal and external factors

Q. What technologies are lacking to improve your company product or services?

A. artificial intelligence, cyber security, high performance computing

Q. Do you see a different need for technology specialists or technology/product generalists in the future?

A. no … these are strictly related

Q. What current opportunities do your employees have for learning and gaining future skills?

A. agreement with general purpose provider of education on line, like Coursera

The launch of a new crucial initiative (Corporate Labs) devoted to base research on technologies (up to TRL 4)

Q. What aspects do you think create a gap between the current defence-oriented educational programmes and new technologies?

A. bad recognition, importance and impact of defence sector on society

Q. What defence applications/subfields should be prioritised?

A. Space technologies and cyber security / resilience

Educational institution Partners

Q. What technologies are taught at your institute and how are they relevant for defence?

A.

Q. What EQF levels is the institute teaching?

A.

Q. What are the formats of the courses taught at the institute?

A.

Q. What pre-skills/experiences do students need?

A.

Q. Are your current teachers ready to accommodate the special learning needs of post-secondary students?

A.

Q. What aspects do you think create a gap between the current defence-oriented educational programmes and new technologies?

A.

Q. What defence applications/subfields should be prioritised?

A.

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

QUESTIONNAIRE

Skills & Technology mapping

in

AI & robotics, Cybersecurity and C4ISTAR

Date:

- 16/03/2020: 1st draft;

Authors: Aalborg University
Revised:
Validated:
Approved:

Industrial partners

Q. What technologies do your company specialize in?

A.

Q. What defence applications and subfields do your company specialised in?

A.

Q. What future skills and personnel profiles are required in your company to improve your products and services?

A. For AI, we will need the following skills and profiles:

- Key foundational skill-set: Being able to frame an AI problem (translating a business use case into a question AI can solve and identify the pre-requisites needed for AI to be able to solve it), avoiding data bias and ensuring data compliance
- Key foundational skill-set: AI methods and tools, such as Machine Learning, Deep Learning, Convolutional Neural Networks, Tensorflow, Keras, PyTorch and any other new toolset appearing
- Specialised skill-set: Computer Vision/ Image Recognition
- Specialised skill-set: Deep Reinforcement Learning
- Specialised skill-set: Natural Language Processing/ Conversational Assistance
- Specialised skill-set: Anomaly Detection/ Time Series
- Specialised skill-set: Knowledge Extraction
- Specialised skill-set: Advanced Optimisation
- Specialised skill-set: Machine Learning Engineering

For Robotics, we will need the following skills and profiles:

- In close link with AI, automation (based on most lively Deep Reinforcement Learning and Computer Vision)
- UX/UI Design
- Robotics operators (ability to operate and program robotics solutions for our production processes)
- Industrial architects (ability to translate an industrial process into integrated digital solutions incl.

robotics)

For engineering:

• Secured connectivity: Cloud based architectures. 4&5G mobile networks. Multibands high data rate, Secure and multibands Modems. Quantum Computing & Coms.

• Electronics, digital playloads: Software and Firmware Engineering.

• Electrification: Energy storage/ batteries. Integrated Power and Thermal Management. Electrical Systems. High power Electronics

• Materials, structures and dynamics: Metallic Materials.

• Military Competences: Simulation. Cyber security. Advanced sensor data & Info fusion

Q. Do your company already have these necessary skills?

A.

Q. Which skill gaps cause the most concern in your company?

A. In current workforce, our biggest concern is that the global data literacy is very low. Our employees do not understand how to take the most out of the data we have and gather and have therefore unrealistic expectations towards Data Science and AI. Globally, we are lacking Software developers with a strong DevOps skillset that are able to translate promising Proof of Concept projects into large-scale, usable applications/ software/ platforms.

With regards to robotics, most of our blue collar populations still needs to be trained on operating robots incl. being able to program and solve minor technical problems.

Q. What causes these skill gaps?

A. For Data Literacy, it is linked to the fact that data literacy is a quite recent skillset that has not been taught at school/ university. For Software Developers, the main root-cause is that in the past we did not consider this to be a core activity and therefore heavily relied on buying those skills. Now that the demand for developers increases globally, we are facing a skill gap internally. For Robotics, it is linked to the fact that robotics is not yet part of the apprenticeship programme/ curriculum of our blue collar workers.

Q. What technologies are lacking to improve your company product or services?

A.

Q. Do you see a different need for technology specialists or technology/product generalists in the future?

A. Yes, we will indeed need technology specialists who are able to build/ create and combine different AI/ robotics solutions, e.g.

- Industrial Architects,
- AI specialists, such as Computer Vision specialists
- Machine Learning Engineers
- Developers with DevOps skills

But more largely, we will need our workforce to be able to apply/ reuse existing solutions for a given use case or purpose, e.g.

- Framing an AI problem and being able to pick the most efficient/ accurate AI solution(s)
- Operate an automated system/ robot autonomously

Q. What current opportunities do your employees have for learning and gaining future skills?

A.

Q. What aspects do you think create a gap between the current defence-oriented educational programmes and

new technologies?

A. No European or International cross programs existing. Airbus has created with Universities some specific programs to answer our own demand (e.g in Spain Airframe master or the Aircraft systems integration Master with Carlos III University). Modern learning solutions anticipating future skills are highly needed in Europe: we are sometimes using US learning company as Udacity to answer our learning necessities. A benchmarking with other type of industries could be a good approach to find correct learning solutions. E.g Ecole 42 in the telecom industry.

Q. What defence applications/subfields should be prioritised?

A.

Educational institution Partners

Q. What technologies are taught at your institute and how are they relevant for defence?

A.

Q. What EQF levels is the institute teaching?

A.

Q. What are the formats of the courses taught at the institute?

A.

Q. What pre-skills/experiences do students need?

A.

Q. Are your current teachers ready to accommodate the special learning needs of post-secondary students?

A.

Q. What aspects do you think create a gap between the current defence-oriented educational programmes and

new technologies?

A.

Q. What defence applications/subfields should be prioritised?

A.

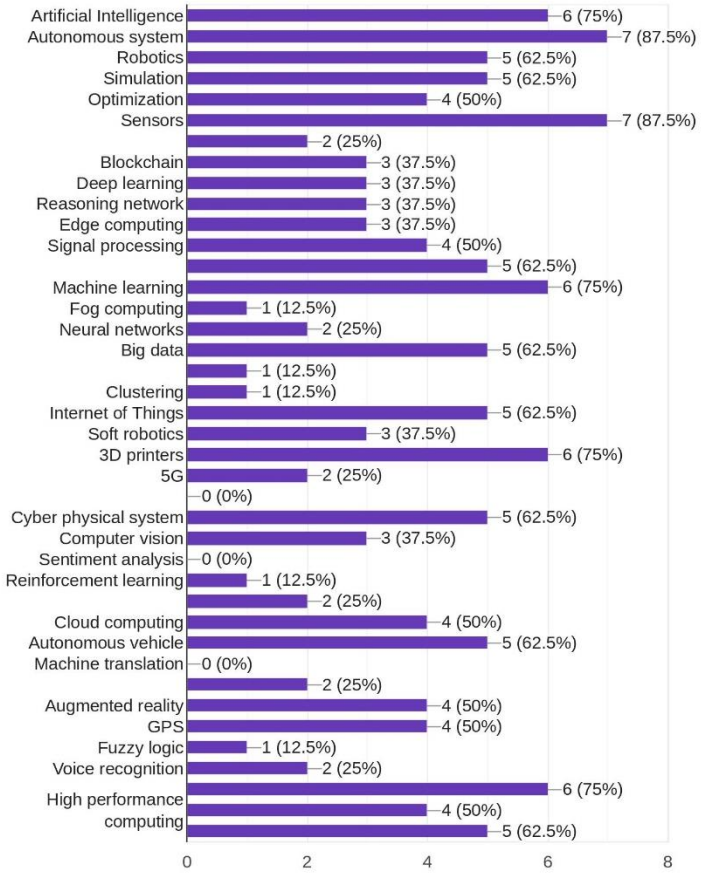
With the support of the Erasmus+ Programme of the European Union

Technology Roadmap

Survey 2

Among the following, select the technologies that you believe are relevant for your company or the defence sector in general.

8 responses



Are there are any technologies missing within the fields of AI, robotics and autonomous systems? If yes, propose additional technologies that you believe are or will be relevant for the defence sector. Leave blank if there are no additional suggestions.

3 responses

Automation, Industrial automation, Cyber security

Cyber & physical security, product safety

- cyber security / communication security
- satellite link and communication
- additive manufacturing

Appendix 2. Technologies description – AAU and PRZ team

This appendix, in Table 8, lists the technologies from expert knowledge identified by AAU and PRZ team for the robotics, AI and autonomous-systems domain.

Technology	Possible application	Possible military application Possible defence industry application	Source
5G communication technology	Communication with and between ground and air autonomous vehicles / devices Range: < 10 m for 60 GHz WiFi, tens of kilometers with fixed links	For sending commands and receiving data to/from Unmanned Vehicles, smart weapons, smart devices etc. Necessary for integration sensors requiring high speed for transmitting the data (up to 20 Gbps) such as LIDARS.	Marko Höyhtyä , Jyrki Huusko , and Markku Kiviranta, Kenneth Solberg , and Juha Rokka, Connectivity for Autonomous Ships: Architecture, Use Cases, and Research Challenges 2017 International Conference on Information and Communication Technology Convergence (ICTC) Yang, Y., & Hua, K. (2019). Emerging technologies for 5G-enabled vehicular networks. IEEE Access, 7, 181117-181141.
LTE/4G	Communication with and between ground and air autonomous vehicles / devices Range: typically < 2 km up to 70 km with directional antennas	For sending commands and receiving data to/from Unmanned Vehicles, smart weapons, smart devices etc. Max bit rate: 75/300 Mbps for Upload/Download	Marko Höyhtyä , Jyrki Huusko, and Markku Kiviranta, Kenneth Solberg , and Juha Rokka, Connectivity for Autonomous Ships: Architecture, Use Cases, and Research Challenges 2017 International Conference on Information and Communication Technology Convergence (ICTC) Chen, W., Niu, K., Wu, D., Zhao, D., Wang, L., & Zhang, D. (2019, September). A contactless gesture interaction system using LTE (4G) signals. In Adjunct Proceedings of the 2019 ACM International Joint Conference on Pervasive and Ubiquitous Computing and Proceedings of the 2019 ACM International Symposium on Wearable Computers (pp. 260-263).
WiFi	Communication with and between ground and air autonomous vehicles / devices Range typically < 100 m, up to 10 km with fixed service	For sending commands and receiving data to/from Unmanned Vehicles, smart weapons, smart devices etc. Max bit rate: 600 Mbps	Marko Höyhtyä , Jyrki Huusko , and Markku Kiviranta, Kenneth Solberg , and Juha Rokka, Connectivity for Autonomous Ships: Architecture, Use Cases, and Research Challenges 2017 International Conference on Information and Communication Technology Convergence (ICTC) Sun, A., Gong, W., Shea, R., Liu, J., Liu, X. S., & Wang, Q. (2017, October). Drone privacy shield: A WiFi based defense. In 2017 IEEE 28th Annual International Symposium on Personal, Indoor, and Mobile Radio Communications (PIMRC) (pp. 1-5). IEEE. Hooper, M., Tian, Y., Zhou, R., Cao, B., Lauf, A. P., Watkins, L., ... & Alexis, W. (2016, November). Securing commercial wifi-based uavs from common security attacks. In MILCOM 2016-2016 IEEE Military Communications Conference (pp. 1213-1218). IEEE.
Layered Control Technique	This technique has been used in control autonomous systems ranging from underwater	Control technique for planned control of Military Unmanned Vehicles.	Gat, E., “On Three-layer Architectures,” in Artificial Intelligence and Mobile Robots, AAAI Press, pp. 195–210 (1997). Albus, J., and Meystel, A., “A Reference Model Architecture for Design and

Technology	Possible application	Possible military application Possible defence industry application	Source
	vehicles to exploratory spacecrafts.	An elaborated version has even been proposed as a standard for intelligent manufacturing systems.	Implementation of Intelligent Control in Large and Complex Systems," Int. J. Intell. Control Syst. 1(1), 15–30 (1996
Model-Based Reasoning	This control technique is used in expert systems based on a model of the physical world. Such systems allow for performing diagnosis or a prediction.	An expert system helping in issuing correct commands for troops in combat situation. An expert system finding optimal design parameters for a new weapon tailored for specific task.	Newton S. Lee (1990). "A computational paradigm that integrates rule-based and model-based reasoning in expert systems". *International Journal of Intelligent Systems*. Wiley. **5** (2): 135—151 Niederlinski, A (2001). "An expert system shell for uncertain rule-and model based reasoning". *Methods of Artificial Intelligence in Mechanics and Mechanical Engineering AIMech*. Tazl, O. A., & Wotawa, F. (2019, July). Using model-based reasoning for enhanced chatbot communication. In International Conference on Industrial, Engineering and Other Applications of Applied Intelligent Systems (pp. 791-798). Springer, Cham. Krichene, A., Kacprzynski, GJ. (2004). Generated model-based reasoning architectures through dynamic simulation. ISAS/CITSA 2004: International Conference on Cybernetics and Information Technologies, Systems and Applications and 10th International Conference on Information Systems Analysis and Synthesis, Vol 1, Proceedings: COMMUNICATIONS, INFORMATION TECHNOLOGIES AND COMPUTING. Edited by: Chu, HW; Aguilar, J; Ferrer, J., Pages: 326-331.
Reactive Behavior Technique	A simple yet effective technique used in autonomous systems such as autonomous vacuum cleaners to safely avoid obstacles.	This technique allows for implementing broad fail-safe system in weapons and smart ammunition. This generally consists of a periodic test to see that a system telemetry vector lies within a desired operating envelope. If the test fails, the system is immediately commanded to a known safe state.	Brooks, R. A., A Robust Layered Control System for a Mobile Robot, Tech. Rep. A. I., Memo 864, MIT, Artificial Intelligence Laboratory (Sep 1955)
Swarm Intelligence (type of Reactive Behavior distributed autonomy)	Mimicking behaviors of social animals using robotic swarms. Collective robotic assembly of structures. Foraging of recourses etc.	Autonomous distributed sensor arrays, detecting enemy movement. Autonomous demining swarms. Swarm of scouting drones. Autonomous swarms designed to build defence structures.	Programmable self-assembly in a thousand-robot swarm Michael Rubenstein, Alejandro Cornejo, Radhika Nagpal *SCIENCE* 15 AUG 2014 : 795-799 Clifford, J., Neighbors, J., & Towhidnejad, M. (2018, May). An integrated swarm intelligence simulation for resilient autonomous systems. In Disruptive Technologies in Information Sciences (Vol. 10652, p. 1065212). International Society for Optics and Photonics. Bogue, R. (2008). Swarm intelligence and robotics. Industrial Robot: An International Journal, 35(6), 488-495.

Technology	Possible application	Possible military application Possible defence industry application	Source
AI accelerator application-specific integrated circuit , Tensor Processing Unit, Nvidia Drive PX	Hardware allowing implementation of autonomous behaviour, especially based on artificial intelligence (Artificial neural networks) Autonomous cars, unmanned air vehicles (UAV) etc.	Hardware enabling usage of artificial intelligence in autonomous vehicles. Autonomous tanks, planes, ships etc. Production optimization and artificially augmented planning in military factories.	Abdul Hamid, Umar Zakir & Pushkin, Konstantin & Zamzuri, Hairi & Gueraiche, Djahid & Abdul Rahman, Mohd Azizi. (2016). Current Collision Mitigation Technologies for Advanced Driver Assistance Systems – A Survey. PERINTIS eJournal. 6. 78-90.
Graphics processing unit GPU	Of shelf hardware allowing implementation of artificial intelligence algorithms. Autonomous vehicles, expert systems.	Autonomous tanks, planes, ships, air defence etc. Expert systems in military factories.	Vasilache, Nicolas & Johnson, Jeff & Mathieu, Michael & Chintala, Soumith & Piantino, Serkan & Lecun, Yann. (2014). Fast Convolutional Nets With fbfft: A GPU Performance Evaluation. Arxiv.
Field Programmable Gate Array, (FPGA)	FPGAs provide better performance than GPUs in DeepLearning and other specific artificial intelligence algorithms. Autonomous vehicles, expert systems.	Autonomous tanks, planes, ships, air defence etc. Expert systems in military factories.	Lacey, Griffin & Taylor, Graham & Areibi, Shawki. (2016). Deep Learning on FPGAs: Past, Present, and Future. Zhang, JL, Qu, G. (2019). Recent Attacks and Defenses on FPGA-based Systems. ACM TRANSACTIONS ON RECONFIGURABLE TECHNOLOGY AND SYSTEMS, vol. 12, issue 3, SI. Jang, M., Ryu, Y., & Park, H. (2018, May). A FPGA-Based scheme for protecting weapon system software technology. In International Conference on Computational Science and Its Applications (pp. 148-157). Springer, Cham.
Non FPGA Embedded Systems	Small form factor computers allowing for design simple autonomous systems, smart devices with limited autonomous behaviour. Smartphone, Smart home, smart washing machine etc.	Smart weapons, smart bombs, small autonomous drones. Personal combat situation analyzer etc.	Reddy, Bhargava & Kim, Ye-Hoon & Yun, Sojung & Seo, Chanwon & Jang, Junik. (2017). Real-Time Driver Drowsiness Detection for Embedded System Using Model Compression of Deep Neural Networks. 438-445. 10.1109/CVPRW.2017.59.
Natural Language Generation	To communicate information	To communicate instructions	https://www.educba.com/artificial-intelligence-technology/ Foster, M. E. (2019). Natural language generation for social robotics: opportunities and challenges. Philosophical Transactions of the Royal Society B, 374(1771), 20180027.
Image Semantic Segmentation	To detect object in an image, Self-driving vehicles, Face detection	Face detection	Liu, X., Deng, Z., & Yang, Y. (2019). Recent progress in semantic image segmentation. Artificial Intelligence Review, 52(2), 1089-1106.
Image Classification	Sorting images, locating images with faults	Finding similarity between pictures, eg. pictures of terrain or satellite pictures	https://towardsdatascience.com/wtf-is-image-classification-8e78a8235acb Bai, X., Xue, R., Wang, L., & Zhou, F. (2019). Sequence SAR Image Classification Based on Bidirectional Convolution-Recurrent Network. IEEE Transactions on Geoscience and Remote Sensing, 57(11), 9223-9235.

Technology	Possible application	Possible military application Possible defence industry application	Source
Image Instance Segmentation	Face recognition, Fingerprint recognition, Iris recognition, Self-driving vehicles	Face recognition, Fingerprint recognition, Iris recognition, Self-driving vehicles	Romera-Paredes, B., & Torr, P. H. S. (2016, October). Recurrent instance segmentation. In European conference on computer vision (pp. 312-329). Springer, Cham. - https://towardsdatascience.com/instance-segmentation-using-mask-r-cnn-7f77bdd46abd - https://engineering.matterport.com/splash-of-color-instance-segmentation-with-mask-r-cnn-and-tensorflow-7c761e238b46
Content-based image retrieval	To search for images similar to given picture, Internet search based on content of an image	Finding images similar to given picture	Ahmed, K. T., Ummesafi, S., & Iqbal, A. (2019). Content based image retrieval using image features information fusion. Information Fusion, 51, 76-99.
Object Co-segmentation	Video content analysis and segmentation	CCTV	Li, W., Jafari, O. H., & Rother, C. (2018, December). Deep object co-segmentation. In Asian Conference on Computer Vision (pp. 638-653). Springer, Cham.
Long short-term memory	Robot control, Time series prediction, Speech recognition	Handwriting recognition, Human action recognition, Time series anomaly detection, Short-term traffic forecast	Hochreiter, S., & Schmidhuber, J. (1997). Long short-term memory. Neural computation, 9(8), 1735-1780. - https://towardsdatascience.com/illustrated-guide-to-lstms-and-gru-s-a-step-by-step-explanation-44e9eb85bf21
Part-of-speech tagging	To recognize parts of a sentence which play specific role	To recognize specific parts of sentence in intelligence	https://medium.com/analytics-vidhya/pos-tagging-using-conditional-random-fields-92077e5eaa31 Kobyliński, Ł., & Kieraś, W. (2016, April). Part of speech tagging for Polish: State of the art and future perspectives. In International Conference on Intelligent Text Processing and Computational Linguistics (pp. 307-319). Springer, Cham.
Terminology extraction	To automatically extract relevant terms from a given set of words	To access information stored in documents and texts	Pazienza, M. T., Pennacchiotti, M., & Zanzotto, F. M. (2005). Terminology extraction: an analysis of linguistic and statistical approaches. In Knowledge mining (pp. 255-279). Springer, Berlin, Heidelberg. - Mollá, D., Schwitter, R., Rinaldi, F., Dowdall, J., & Hess, M. (2003). NLP for answer extraction in technical domains. Proceedings of EACL, USA.
Text-to-speech	Reading a document by a program/ computer, Reading websites for visually impaired people		Taylor, P. (2009). Text-to-speech synthesis. Cambridge university press. - Ren, Y., Ruan, Y., Tan, X., Qin, T., Zhao, S., Zhao, Z., & Liu, T. Y. (2019). Fastspeech: Fast, robust and controllable text to speech. In Advances in Neural Information Processing Systems (pp. 3165-3174).
Speech recognition	To recognize spoken words, then convert them to text.		Chan, W., Jaitly, N., Le, Q. V., Vinyals, O., & Shazeer, N. M. (2020). U.S. Patent No. 10,540,962. Washington, DC: U.S. Patent and Trademark Office. -

Technology	Possible application	Possible military application Possible defence industry application	Source
			van den Oord, A. G. A., Dieleman, S. E. L., Kalchbrenner, N. E., Simonyan, K., Vinyals, O., & Espeholt, L. (2019). U.S. Patent Application No. 16/209,661.
Voice recognition	To identify a person based on their voice.	Intelligence, security	Eljawad, L., Aljamaeen, R., Alsmadi, M., Almarashdeh, I., Abouelmagd, H., Alsmadi, S., ... & Alazzam, M. (2019). Arabic Voice Recognition Using Fuzzy Logic and Neural Network. ELJAWAD, L., ALJAMAEEN, R., ALSMADI, MK, AL-MARASHDEH, I., ABOUELMAGD, H., ALSMADI, S., HADDAD, F., ALKHASAWNEH, RA, ALZUGHOUL, M. & ALAZZAM, MB, 651-662. - Kim, Dami. "Deeplearning method for voice recognition model and voice recognition device based on artificial neural network." U.S. Patent Application No. 16/567,880.
Discourse/ sentiment analysis	To analyse what people think about specific topic. What they like or not.	Intelligence, Emotion recognition	Misnikov, Y., & Filatova, O. (2019). Testing the Applicability of Training Recurrent Neural Networks for Analyzing Online Policy Discourses in Russia. EGOV-CeDEM-ePart 2019, 119. - Kraus, M., & Feuerriegel, S. (2019). Sentiment analysis based on rhetorical structure theory: Learning deep neural networks from discourse trees. Expert Systems with Applications, 118, 65-79.
Word sense disambiguation	To identify which sense of a word is used in a sentence	Cryptography, Intelligence, Analytics	Yarowsky, D. (1995, June). Unsupervised word sense disambiguation rivaling supervised methods. In 33rd annual meeting of the association for computational linguistics (pp. 189-196). - Wang, Y., Wang, M., & Fujita, H. (2020). Word sense disambiguation: a comprehensive knowledge exploitation framework. Knowledge-based Systems, 190, 105030. - Scarlini, B., Pasini, T., & Navigli, R. (2020). SENSEMBERT: Context-Enhanced Sense Embeddings for Multilingual Word Sense Disambiguation. In Proc. of AAAI.
Topic segmentation and recognition	To recognize and analyse topics of a document	To analyse documents	Yamamoto, N., Ogata, J., & Ariki, Y. (2003). Topic segmentation and retrieval system for lecture videos based on spontaneous speech recognition. In Eighth European Conference on Speech Communication and Technology. - Mori, G., Ren, X., Efros, A. A., & Malik, J. (2004, June). Recovering human body configurations: Combining segmentation and recognition. In Proceedings of the 2004 IEEE Computer Society Conference on Computer Vision and Pattern Recognition, 2004. CVPR 2004. (Vol. 2, pp. II-II). IEEE. - Arnold, S., Schneider, R., Cudré-Mauroux, P., Gers, F. A., & Löser, A.

Technology	Possible application	Possible military application Possible defence industry application	Source
			(2019). SECTOR: A Neural Model for Coherent Topic Segmentation and Classification. Transactions of the Association for Computational Linguistics, 7, 169-184.
Optical character recognition	Recognition of written words and sentences	To recognize written documents and to digitalize them	Srivastava, S., Priyadarshini, J., Gopal, S., Gupta, S., & Dayal, H. S. (2019). Optical Character Recognition on Bank Cheques Using 2D Convolution Neural Network. In Applications of Artificial Intelligence Techniques in Engineering (pp. 589-596). Springer, Singapore. - Chang, C. C., Arora, A., Perera, L. P. G., Etter, D., Povey, D., & Khudanpur, S. (2019, September). Optical Character Recognition with Chinese and Korean Character Decomposition. In 2019 International Conference on Document Analysis and Recognition Workshops (ICDARW) (Vol. 5, pp. 134-139). IEEE. - Sampath, A. K., & Gomathi, N. (2019). Handwritten optical character recognition by hybrid neural network training algorithm. The Imaging Science Journal, 67(7), 359-373.
Named entity recognition	To locate and classify named entity mentioned in unstructured text into pre-defined categories such as person names, organizations, locations, medical codes, time expressions, quantities, monetary values, percentages, etc.	Intelligence, Research	Lample, G., Ballesteros, M., Subramanian, S., Kawakami, K., & Dyer, C. (2016). Neural architectures for named entity recognition. arXiv preprint arXiv:1603.01360. - Jain, A., Tayal, D. K., Yadav, D., & Arora, A. (2020). Research Trends for Named Entity Recognition in Hindi Language. In Data Visualization and Knowledge Engineering (pp. 223-248). Springer, Cham.
Machine translation	To translate text or speech from one language to another	Translation of text between languages. Intelligence, analytics.	Brown, P. F., Cocke, J., Della Pietra, S. A., Della Pietra, V. J., Jelinek, F., Lafferty, J., ... & Roossin, P. S. (1990). A statistical approach to machine translation. Computational linguistics, 16(2), 79-85. - Cheng, Y. (2019). Semi-supervised learning for neural machine translation. In Joint Training for Neural Machine Translation (pp. 25-40). Springer, Singapore. - Barrault, L., Bojar, O., Costa-jussà, M. R., Federmann, C., Fishel, M., Graham, Y., ... & Monz, C. (2019, August). Findings of the 2019 conference on machine translation (wmt19). In Proceedings of the Fourth Conference on Machine Translation (Volume 2: Shared Task Papers, Day 1) (pp. 1-61).
Virtual Agents	Customer service agent who works remotely and automatically.	Training, teaching	Vaughn, G., Sivakumar, G., & Gopal, V. M. (2020). U.S. Patent Application No. 16/038,332. - Wang, I., Smith, J., & Ruiz, J. (2019, May). Exploring virtual agents for augmented reality. In Proceedings of the 2019 CHI Conference on Human

Technology	Possible application	Possible military application Possible defence industry application	Source
			Factors in Computing Systems (pp. 1-12).
Time-series prediction	Forecasting weather or stock market changes.	Forecasting changes in time-dependent variables important for defence or military.	Weigend, A. S. (2018). Time series prediction: forecasting the future and understanding the past. Routledge. - Hua, Y., Zhao, Z., Li, R., Chen, X., Liu, Z., & Zhang, H. (2019). Deep learning with long short-term memory for time series prediction. IEEE Communications Magazine, 57(6), 114-119.
GPS	To locate the position of the robot To track the robot	To locate the position of the robot in the field To track the robot in the field	Chang Li, Hanxu Sun and Ping Ye, Multi-sensor fusion localization algorithm for outdoor mobile robot. Journal of Physics: Conference Series, Volume 1453, 2019 2nd International Conference on Computer Information Science and Artificial Intelligence (CISAI 2019), 25-27 October 2019, Xi'an, China
Intelligent Systems and Robotics Center (ISRC)	Utilization and protection of industrial and military waste by manipulator	The described system is used for the utilization and checking of waste and nuclear weapons by a 6-axis manipulator	https://www.robotyka.com/teoria.php/teoria.52 Drotning, W., Wapman, W., Fahrenholtz, J., Kimberly, H., & Kuhlmann, J. (1996). System design for safe robotic handling of nuclear materials (No. SAND-96-0485C; CONF-9606123-1). Sandia National Labs., Albuquerque, NM (United States).
A neural scanner (atometry method)	Determination of the shape and stoichiometry of tested objects. This makes it possible to detect, for example, mines or even small amounts of hazardous materials hidden in vehicles, luggage	Detection of explosives, demining the area	Silarski, M., & Moskal, P. Atometria jako metoda wykrywania substancji niebezpiecznych. Foton, 112, s.15-22. 2011
Pyrotechnic robots **Pyrotechnic ejectors (CSL Vulkan)**	Use in army industry Mounting to various types of robots to perform neutralization tasks (pyrotechnic ejectors)	They are used to identify the area, their main task is to enable the robot operator to carry out IED neutralization procedures from a distance, without having to risk their own lives Specialized EOD tools, whose task is to launch a projectile with such speed and precision to break the IED device into completely or partially deprive them of combat qualities	Zalewski, D. (2017). Specjalistyczne pododdziały wojsk inżynieryjnych Sił Zbrojnych Rzeczypospolitej Polskiej przeznaczone do zwalczania improwizowanych urządzeń wybuchowych. Obronność–Zeszyty Naukowe Wydziału Zarządzania i Dowodzenia Akademii Sztuki Wojennej, (4 (24)). Bitonneau, D., Moulières-Seban, T., Dumora, J., Ly, O., Thibault, J. F., Salotti, J. M., & Claverie, B. (2017, December). Design of an industrial human-robot system through participative simulations—Tank cleaning case study. In 2017 IEEE/SICE International Symposium on System Integration (SII) (pp. 1-8). IEEE.
A crawler system	Use in a mobile robot (Robot PIAP GRYF)	Dedicated to operations in difficult external conditions such as deep snow or sand, the track system reduces unit pressure on the ground, so	https://www.antyterroryzm.com/portfolio-posts/gryf-snieg-piach/ Grabania, M. Ł., Holota, M., Kurpas, M., & Olek, J. (2012). Modułowa platforma gąsienicowa ANDERS. Szybkobieżne Pojazdy Gąsienicowe (30) nr, 2.

Technology	Possible application	Possible military application Possible defence industry application	Source
		that the robot does not get buried in the ground, and the track tensioning system together with the cleaning system ensures that snow and sand will not clog the chassis	Inoue, T., Takagi, K., & Shiosawa, T. (2011, June). Experiments of flipper type crawler system at sea to verify running performance on sandy or irregular steep terrain seafloor. In OCEANS 2011 IEEE-Spain (pp. 1-5). IEEE.
A laser scanner	Use in a mobile robot	Creating a 2D map that allows the identification of objects on the stage for the mobile robot Classification of the substrate based on data from the laser scanner in which the robot is equipped	Quemelli, M. B., & Brandão, A. S. (2020). Handling and pushing objects using unmanned guided vehicles. Robotics and Computer-Integrated Manufacturing, 63, 101913. Undak, M., & Siemiątkowska, B. (2010). Zastosowanie sieci komórkowych do tworzenia semantycznych map otoczenia robota mobilnego. Pomiary Automatyka Robotyka, 14, 305-313.
The Atos Core 3D scanner	Use in manipulators	Geometrical inspection of an aircraft engine turbine stator segment employing the ABB IRB 1600 robot, equipped with the Atos Core 3D scanner and interfaced with the Atos Professional software suite.	Burghardt, A., Kurc, K., Szybicki, D., Muszyńska, M., & Szczęch, T. (2017). Robot-operated inspection of aircraft engine turbine rotor guide vane segment geometry. Tehnički vjesnik, 24(Suppl. 2), pp.345-348. Burghardt, A., Kurc, K., & Szybicki, D. (2016). Robotic automation of the turbo-propeller engine blade grinding process. In Applied Mechanics and Materials (Vol. 817, pp. 206-213). Trans Tech Publications, Switzerland.
Platforma Topomap	Use in a mobile robotic platform	Robot navigation, robot path planning	F. Blochliger, M. Fehr, M. Dymczyk, T. Schneider and R. Siegwart, "Topomap: Topological Mapping and Navigation Based on Visual SLAM Maps," *2018 IEEE International Conference on Robotics and Automation (ICRA)*, Brisbane, QLD, 2018, pp. 3818-3825.
3D printers	Production of elements of any shape and application	Production of spare parts or soft robots (flexible and able to squeeze into tight gaps) - using mechanisms from dielectric elastomers Servicing and modernizing fighter aircraft to meet NATO requirements. Production of spare parts for Boeing	Haghiashtiani, G., Habtour, E., Park, S. H., Gardea, F., & McAlpine, M. C. (2018). 3D printed electrically-driven soft actuators. Extreme Mechanics Letters, 21, pp.1-8. Paul Davidson, "3-D printing could remake U.S. manufacturing," USA Today (July 10, 2012) http://usatoday30.usatoday.com/money/industries/manufacturing/story/2012-07-10/digitalmanufacturing/56135298/1 https://stal.elamed.pl/material%5B29789%5D?fbclid=IwAR2alysUa7qK8Kzg7x77-gvfB8P72R0aDQw8uutza93U3c8z1LGnfd4g6l4
Multimove	Used in a robotic station	Machining of components for combat aircraft engines used in the military industry	Burghardt, A., Szybicki, D., Kurc, K., Muszyńska, M., & Mucha, J. (2017). Experimental study of Inconel 718 surface treatment by edge robotic deburring with force control. Strength of Materials, 49(4), pp.594-604.
IP-based vision system	Designing hardware, firmware and software for a mobile robot	Image recognition measured when distance changes and ambient luminance changes.	A. A. Bandala and E. P. Dadios, "Development and design of mobile robot with IP-based vision

Technology	Possible application	Possible military application Possible defence industry application	Source
	capable of sending video information and receiving commands from a checkpoint	Measuring the accuracy of mobile robot motion	system," TENCON 2012 IEEE Region 10 Conference, Cebu, 2012, pp. 1-6.

Table 8 - List of technologies from expert knowledge.

Appendix 3. Results of the technologies classification – AAU and PRZ team

This appendix contains, in Figure 5, a visualization of the evolution of the number of papers published by the selected technologies between the years 2009 and 2018, as explored by AAU and PRZ team for technologies classification in robotics, AI & autonomous-system domain. This is an additional output.

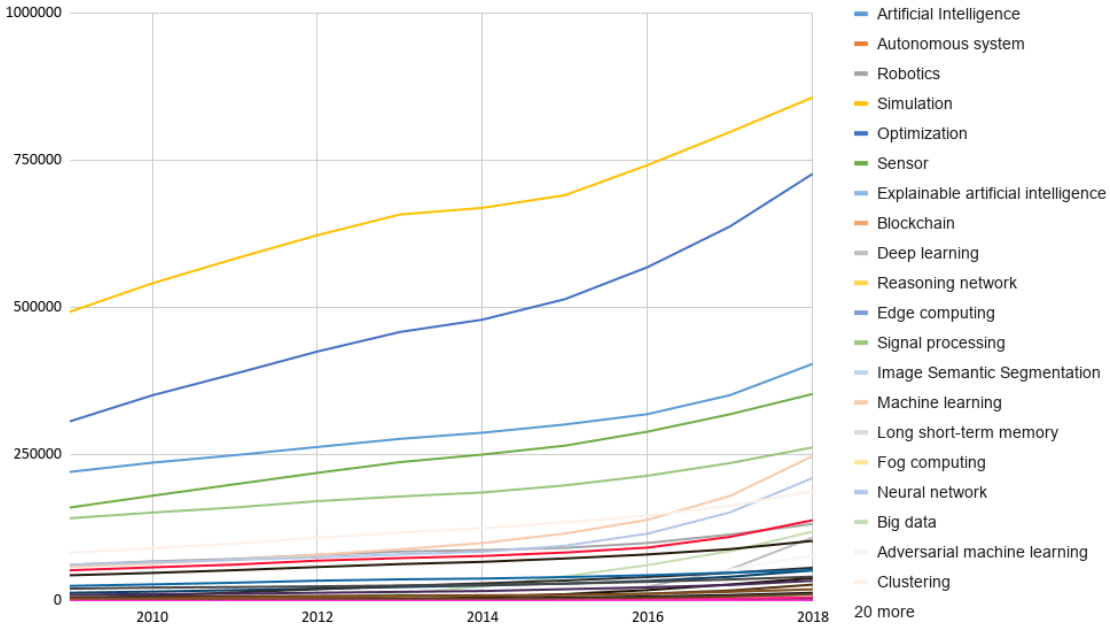


Figure 5 - Evolution of number of papers referencing the technologies.

Appendix 4. Results of the relevance matrix– AAU and PRZ team

This appendix contains, in Figure 6, the initial version of the Relevance matrix defined by AAU and PRZ team for the description of the relationships between the applications and the technologies related to robotics, AI & autonomous-system domain. This version is preceding the final one, obtained by expert judgment, as explained in Paragraph 4.1.3 “Relevance matrix: robotics, AI & autonomous-system domain”.

The relevance matrix was generated based on the number of papers containing both the technology keyword and the application. Afterwards, the results are normalized in the interval [0,10]. The relevance matrix is reported in Figure 6, where dark and light green represent high and low scores respectively.

keyword	Mission planning	Mission control	Reconnaissance	Surveillance	Routing	Scheduling	Assignment	Coverage	Rescue	Target tracking	Combat simulation	Military vehicle manufacturing	Missile guidance	Anomaly detection	Trajectory tracking	Path planning	Space technologies	Cyber security	Cyber resilience	Aeronautics	land armours	Naval	Underwater	Satellite	Weapons	Fighter aircrafts
Artificial Intelligence	8	8	7	7	6	6	7	7	6	7	7	6	6	6	5	7	8	7	5	5	0	7	6	6	7	4
Autonomous system	8	9	8	8	6	6	7	7	6	8	8	6	6	5	6	7	8	6	5	6	0	7	7	7	7	4
Robotics	7	7	6	7	5	5	5	6	5	6	6	5	5	4	5	6	7	5	3	4	0	6	6	6	6	3
Simulation	9	10	8	9	7	7	8	8	7	8	10	7	7	6	7	8	9	7	6	7	0	9	7	8	9	5
Optimization	8	9	8	8	7	7	7	8	6	8	8	7	6	6	6	7	8	6	5	7	0	8	6	7	8	5
Sensor	9	9	8	9	7	7	7	8	7	9	8	7	7	7	7	8	9	7	5	7	0	8	7	8	8	5
Explainable artificial intelligence	4	4	3	4	1	1	3	3	2	3	3	2	1	1	0	3	4	4	3	0	0	3	2	2	3	0
Blockchain	1	1	0	2	1	0	0	1	0	2	0	0	0	1	1	0	2	2	0	0	0	0	0	1	1	0
Deep learning	7	7	6	7	5	5	6	6	5	6	7	5	6	5	5	6	7	6	5	5	0	6	5	6	7	4
Reasoning network	7	8	7	7	6	6	7	7	6	7	7	5	6	5	5	7	7	6	4	5	0	7	5	6	7	4
Edge computing	7	7	6	7	6	5	6	6	5	6	7	6	5	5	5	6	7	6	4	6	0	6	5	6	6	4
Signal processing	8	8	8	9	6	6	7	8	6	8	8	6	6	6	7	7	8	6	4	6	0	8	7	8	8	5
Image Semantic Segmentation	3	3	3	3	3	2	3	3	3	3	3	3	3	2	1	3	3	2	1	2	0	3	2	3	3	1
Machine learning	8	8	7	7	6	6	6	7	6	7	7	6	6	5	6	7	8	6	5	5	0	7	6	6	7	4
Fog computing	5	5	5	5	4	4	4	5	4	5	5	4	5	3	4	5	5	3	1	4	0	5	4	4	5	3
Neural network	7	7	6	7	5	6	6	6	5	6	7	5	5	5	5	6	7	5	4	5	0	6	5	6	6	4
Big data	8	8	7	8	6	6	7	7	6	7	7	6	6	6	6	7	8	7	5	6	0	7	6	7	7	5
Adversarial machine learning	5	5	4	5	3	4	4	4	3	4	4	4	4	4	3	4	5	4	4	3	0	4	3	4	5	2
Clustering	6	6	5	6	5	5	5	6	4	6	6	4	4	4	4	5	6	5	3	4	0	6	4	5	5	3
Internet of Things	7	7	6	7	6	6	6	6	5	6	7	5	6	5	5	6	7	6	5	5	0	7	5	6	7	4
Soft robotics	5	5	5	5	4	4	4	5	4	5	5	4	4	3	3	5	5	4	2	4	0	5	4	5	5	1
3D printers	3	3	3	3	3	2	2	3	3	3	3	3	3	1	2	3	3	1	0	2	0	3	2	3	3	0
5G	4	5	4	4	3	3	2	3	3	4	4	3	3	2	3	4	5	2	1	3	0	3	3	4	4	1
Object Co-segmentation	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0
Cyber physical system	7	7	5	6	5	5	5	6	5	6	6	4	5	4	4	6	7	7	6	4	0	6	4	5	6	2
Computer vision	8	8	7	7	6	6	7	7	6	7	8	6	6	5	6	7	8	6	5	6	0	7	6	7	7	4
Sentiment analysis	5	5	4	4	3	1	3	4	3	4	4	2	2	3	2	4	5	4	3	2	0	4	1	3	4	0
Reinforcement learning	6	6	5	5	4	4	5	5	4	5	5	4	4	3	4	5	6	5	3	4	0	5	4	5	6	2
Support vector machine	6	7	6	7	5	5	6	6	5	6	6	5	5	5	5	6	7	5	4	5	0	6	5	6	6	4
Cloud computing	6	7	6	6	5	5	5	6	5	6	6	5	5	4	5	6	7	6	4	5	0	6	4	6	6	3
Autonomous vehicle	8	8	7	8	6	6	6	7	6	7	7	6	6	5	6	7	8	6	5	6	0	7	7	7	7	4
Machine translation	6	7	6	6	5	5	6	6	5	6	6	5	5	4	5	6	7	5	4	5	0	6	4	6	6	3
Natural language processing	7	7	6	7	6	6	6	7	6	7	7	6	6	5	5	7	7	6	5	5	0	7	5	6	7	4
Augmented reality	7	7	6	7	5	6	6	6	6	7	7	5	6	4	5	6	7	5	4	5	0	7	5	6	7	4
GPS	7	8	7	8	6	5	6	7	6	7	7	5	6	5	6	7	7	5	3	5	0	6	6	7	7	4
Fuzzy logic	6	6	5	6	4	5	5	5	4	5	6	4	5	4	4	5	6	4	3	4	0	5	4	5	6	3
Voice recognition	7	7	6	6	5	5	6	6	5	6	6	5	5	4	4	6	7	5	3	4	0	6	4	5	6	4
Human Machine Interaction	8	8	7	7	6	6	7	7	6	7	8	6	6	5	6	7	8	6	5	5	0	7	6	6	7	4
High performance computing	8	8	7	8	6	6	7	7	6	7	8	6	6	6	6	7	8	7	5	6	0	7	6	7	7	4
Structures and Materials	7	8	7	7	5	6	6	7	6	7	8	7	6	5	5	6	8	5	4	6	1	7	5	7	7	5

Figure 6 - First version of Relevance matrix.

It is important to keep in mind that an association between two keywords does not necessarily imply the relevance of the technology for the defence application. Therefore, the Relevance matrix is revised by experts to determine which pair of technology-applications are relevant in the defence sector, in the specific case of robotics, AI & autonomous-system domain.

In this version, reported in Figure 7, the blue cells identify relevant relationships between technology and application based on expert judgement.

keyword	Mission planning	Mission control	Reconnaissance	Surveillance	Routing	Scheduling	Assignment	Coverage	Rescue	Target tracking	Combat simulation	Military vehicle manufacturing	Missile guidance	Anomaly detection	Trajectory tracking	Path planning	Space technologies	Cyber security	Cyber resilience	Aeronautics	land armours	Naval	Underwater	Satellite	Weapons	Fighter aircrafts
Artificial Intelligence	8	8	7	7	6	6	7	7	6	7	7	6	6	6	5	7	8	7	5	5	0	7	6	6	7	4
Autonomous system	8	9	8	8	6	6	7	7	6	8	8	6	6	5	6	7	8	6	5	6	0	7	7	7	7	4
Robotics	7	7	6	7	5	5	5	6	5	6	6	5	5	4	5	6	7	5	3	4	0	6	6	6	6	3
Simulation	9	10	8	9	7	7	8	8	7	8	10	7	7	6	7	8	9	7	6	7	0	9	7	8	9	5
Optimization	8	9	8	8	7	7	7	8	6	8	8	7	6	6	6	7	8	6	5	7	0	8	6	7	8	5
Sensor	9	9	8	9	7	7	7	8	7	9	8	7	7	7	7	8	9	7	5	7	0	8	7	8	8	5
Explainable artificial intelligence	4	4	3	4	1	1	3	3	2	3	3	2	1	1	0	3	4	4	3	0	0	3	2	2	3	0
Blockchain	1	1	0	2	1	0	0	1	0	2	0	0	0	1	1	0	2	2	0	0	0	0	0	1	1	0
Deep learning	7	7	6	7	5	5	6	6	5	6	7	5	6	5	5	6	7	6	5	5	0	6	5	6	7	4
Reasoning network	7	8	7	7	6	6	7	7	6	7	7	5	6	5	5	7	7	6	4	5	0	7	5	6	7	4
Edge computing	7	7	6	7	6	5	6	6	5	6	7	6	5	5	5	6	7	6	4	6	0	6	5	6	6	4
Signal processing	8	8	8	9	6	6	7	8	6	8	8	6	6	6	7	7	8	6	4	6	0	8	7	8	8	5
Image Semantic Segmentation	3	3	3	3	3	2	3	3	3	3	3	3	3	2	1	3	3	2	1	2	0	3	2	3	3	1
Machine learning	8	8	7	7	6	6	6	7	6	7	7	6	6	5	6	7	8	6	5	5	0	7	6	6	7	4
Fog computing	5	5	5	5	4	4	4	5	4	5	5	4	5	3	4	5	5	3	1	4	0	5	4	4	5	3
Neural network	7	7	6	7	5	6	6	6	5	6	7	5	5	5	5	6	7	5	4	5	0	6	5	6	6	4
Big data	8	8	7	8	6	6	7	7	6	7	7	6	6	6	6	7	8	7	5	6	0	7	6	7	7	5
Adversarial machine learning	5	5	4	5	3	4	4	4	3	4	4	4	4	4	3	4	5	4	4	3	0	4	3	4	5	2
Clustering	6	6	5	6	5	5	5	6	4	6	6	4	4	4	4	5	6	5	3	4	0	6	4	5	5	3
Internet of Things	7	7	6	7	6	6	6	6	5	6	7	5	6	5	5	6	7	6	5	5	0	7	5	6	7	4
Soft robotics	5	5	5	5	4	4	4	5	4	5	5	4	4	3	3	5	5	4	2	4	0	5	4	5	5	1
3D printers	3	3	3	3	3	2	2	3	3	3	3	3	3	1	2	3	3	1	0	2	0	3	2	3	3	0
5G	4	5	4	4	3	3	2	3	3	4	4	3	3	2	3	4	5	2	1	3	0	3	3	4	4	1
Object Co-segmentation	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0
Cyber physical system	7	7	5	6	5	5	5	6	5	6	6	4	5	4	4	6	7	7	6	4	0	6	4	5	6	2
Computer vision	8	8	7	7	6	6	7	7	6	7	8	6	6	5	6	7	8	6	5	6	0	7	6	7	7	4
Sentiment analysis	5	5	4	4	3	1	3	4	3	4	4	2	2	3	2	4	5	4	3	2	0	4	1	3	4	0
Reinforcement learning	6	6	5	5	4	4	5	5	4	5	5	4	4	3	4	5	6	5	3	4	0	5	4	5	6	2
Support vector machine	6	7	6	7	5	5	6	6	5	6	6	5	5	5	5	6	7	5	4	5	0	6	5	6	6	4
Cloud computing	6	7	6	6	5	5	5	6	5	6	6	5	5	4	5	6	7	6	4	5	0	6	4	6	6	3
Autonomous vehicle	8	8	7	8	6	6	6	7	6	7	7	6	6	5	6	7	8	6	5	6	0	7	7	7	7	4
Machine translation	6	7	6	6	5	5	6	6	5	6	6	5	5	4	5	6	7	5	4	5	0	6	4	6	6	3
Natural language processing	7	7	6	7	6	6	6	7	6	7	7	6	6	5	5	7	7	6	5	5	0	7	5	6	7	4
Augmented reality	7	7	6	7	5	6	6	6	6	7	7	5	6	4	5	6	7	5	4	5	0	7	5	6	7	4
GPS	7	8	7	8	6	5	6	7	6	7	7	5	6	5	6	7	7	5	3	5	0	6	6	7	7	4
Fuzzy logic	6	6	5	6	4	5	5	5	4	5	6	4	5	4	4	5	6	4	3	4	0	5	4	5	6	3
Voice recognition	7	7	6	6	5	5	6	6	5	6	6	5	5	4	4	6	7	5	3	4	0	6	4	5	6	4
Human Machine Interaction	8	8	7	7	6	6	7	7	6	7	8	6	6	5	6	7	8	6	5	5	0	7	6	6	7	4
High performance computing	8	8	7	8	6	6	7	7	6	7	8	6	6	6	6	7	8	7	5	6	0	7	6	7	7	4
Structures and Materials	7	8	7	7	5	6	6	7	6	7	8	7	6	5	5	6	8	5	4	6	1	7	5	7	7	5

Figure 7 - Relevance matrix of the robotics, AI & autonomous-system domain.

Appendix 5. Results of the applications identification – UNIPI and UNIBX team

This appendix contains the fully list of applications related to the C4ISTAR domain from which are identified the applications reported in Paragraph 4.2.1 “Application of C4ISTAR domain”. It contains 133 entries:

Agile C2; Air Operation; Air Traffic Control; Airspace Management; Analysis; Analytics; Anomaly Detection; Asset Tracking; Authentication; Automatic Control; Automation; Benchmarking; Blockchain; Cartography; Charting ; Cloud Computing; Clustering; Collection Management; Comint; Command ; Communication; Communications Intelligence; Connect; Content Management; Control; Controls; Conversion; Cryptanalysis; Cryptography; Cyberspace; Data Analysis; Data Communication; Data Definition; Data Exchange; Data Fusion; Data Interchange; Data Management; Data Mining; Data Processing; Data Transfer; Data Transmission; Data Visualization; Decision Maker; Decision Making; Decision Support; Design; Digital Communication; Digitize; Dissemination; Distance Learning; Download; Electronic Commerce; Electronic Data Interchange; Encryption; Engineering Geospatial Mapping; Exchange; Exchange Data; Exchange Information; Experimentation; Exploitation; Filter; Human Intelligence; Human-Computer Interaction; Identification; Imagery; Implementation; Information Exchange; Information Processing; Information Sharing; Innovation; Intelligence; Intelligence Cycle; Intrusion Detection; Knowledge Management; Land Operation; Learning; Logistic; Machine Learning; Maintenance; Make Decisions; Material Management; Messaging; Mission; Mobile Computing; Monitoring; Multiplexing; Multi-Touch; Naval Operation; Navigation; Ncw; Pattern Recognition; Photogrammetry; Planning; Positioning; Predictive Analysis; Processing; Processing Data; Production; Program; Programming; Protection; Quantum Computing; Radiotelephone; Reconnaissance; Remote Control; Remote Monitoring; Remote Sensing; Reporting; Robotics; Sharing Information; Sigint; Signals Intelligence; Simulation; Standard Operating Procedure; Storage; Surveillance; Surveillance Systems; Switching In Telecommunication; Synchronisation; Target Acquisition; Telecommunication Technology; Telegraphy; Tele-Traffic; Testing; Track Management; Training; Transitions; Transmission Of Data; Transmissions; Upload; Virtual Reality; Virtualization; Warfighting.

Appendix 6. Results of the technologies identification – UNIPI and UNIBX team

This appendix contains the fully list of technologies related to the C4ISTAR domain from which are identified the technologies reported in Paragraph 4.2.2 “Classify and rate technologies: C4ISTAR domain. It contains 2030 entries:

3-d display; 3d printing; 3d topographical map; 463l system; 4d dual-axis multi-beam radar; 4g mobile; 4g mobile technologies; 4g networks; 5g network; 5th generation; 5th generation systems; Accounting system; Acoustic-based systems; Acoustic sensors; Acoustic systems; Actions container; Active component; Active electronically scanned array; Actuator; Ad hoc wireless networks; Adapt it; Adapt systems; Adaptive control system; Adaptive network; Adaptive planning; Adaptive systems; Adatp3; Additive manufacturing; Ads-b; Advanced battle management systems; Advanced communications controllers; Advanced defense systems; Advanced digital systems; Advanced field artillery tactical data system; Advanced load carriage system; Advanced manufacturing; Advanced manufacturing systems; Advanced military communication system; Advanced navigation technologies; Advanced networking technologies; Advanced radar sensors; Advanced radar systems; Advanced tactical communications system; Advances field collaboration systems; Adversary information systems; Aerial; Aerial distribution system; Aerospace; Aerospace systems; Aerovironment’s puma ae; Aesa techniques; Agent-based model; Agile c2; Agile methodology; Agile software design and development; Agile systems; Agility maps; Air combat system; Air command systems; Air conditioner; Air control element; Air defence system; Air defense networks; Air defense weapons systems; Air ground surveillance sensors; Air missile systems; Air mobility support system; Air radio systems; Air sensor; Air space surveillance systems; Air surveillance system; Air system; Air systems; Air traffic management systems; Air transportation execution system; Airborne; Airborne radio system; Airborne systems; Aircraft; Aircraft sensor; Aircraft systems; Aircraft weapon observer system; Airplane; Airspace control system; Airspace management system; Airspace surveillance technologies; Alarms; Alarms management; Alat light army helicopters; Alert measurement systems; Alert system; Alerting systems; Alliance ground surveillance system; Allocation system; Ambulance service network; Ambulances; Amoled; Amphibious assault fuel system; An/prc- 154 rifleman radio; Analyse unstructured datasets; Analysis tools; Analytical tools; Analytics; Android; Android devices; Android operating system; Android platform; Android smartphone; Android tablet; Animal-shaped robot; Anomaly detection; Antennae technology; Antennas; Anti-aircraft systems; Anti-drone protection systems; Anti-piracy; Anti-spoofing technologies; Antijamming system; Apar; Apar systems; Apar weapons control system; Application interface module; Application programming interface; Application server; Applied sciences; Architecture dod framework systems; Architecture framework information systems; Architecture system; Arcs; Area network; Area networks; Argus-is; Argus airborne radar system; Argus system; Armament system; Armed drones; Armed vehicles; Armoured reconnaissance and combat vehicle; Arms; Army system; Army tactical missile system; Array technology; Artificial intelligence; Artificial intelligence software; Artificial intelligence technologies; Artillery sensors; Artillery tactical data system; Artillery type radar systems; Assault bulk fuel systems; Assess information; Asset movement management system; Asset validation system; Assistance logistics information system; Assurance gncc global network; Athena® combat management system; Atomic energy detection system; Attack radar system; Attritable systems; Audio translation; Augmented reality; Authoritative data sources; Automated biometric identification system; Automated commercial system; Automated computer; Automated control system; Automated information system; Automated intelligence; Automated machine; Automated reasoning; Automated reasoning tool; Automated sensor; Automated systems; Automated threat recognition; Automatic algorithms; Automatic control; Automatic data processing network; Automatic dependent surveillance – broadcast; Automatic identification system; Automatic identification technology; Automatic test equipment; Automation systems; Automotive control systems; Autonomous agents; Autonomous aircraft; Autonomous battle coordination system; Autonomous biometric systems; Autonomous combat

systems; Autonomous control; Autonomous entity; Autonomous learning systems; Autonomous lethal system; Autonomous lethal weapon system; Autonomous machines; Autonomous network; Autonomous real-time ground ubiquitous surveillance system; Autonomous robot; Autonomous robot warfighting networks; Autonomous systems; Autonomous vehicle; Autonomous warfighting systems; Autonomous weapon system; Autonomous weapons; Auxylium communication system; Avant system; Aviator locator system; Avionics; Avionics systems; Backbone; Backpack computer; Ballistic missile; Ballistic missile defense system; Band channels; Bandwidth ubiquitous networks; Barcodes; Bargaining power; Basemap; Battalion mtcr missile technology; Battery; Battery technologies; Battle management core system; Battle management software; Battle management system fires; Battle space object management; Battlefield command support system; Battlefield information systems; Battlefield management system; Battlefield of things; Battlefield surveillance; Battlefield surveillance system; Battlefield targeting tool; Battlespace data integration mechanisms; Beacon; Big data; Big data analysis; Big data software; Bing; Binocular target acquisition system; Binoculars; Biomechanical; Biometric; Biometric identification; Biometric sensor; Biometric systems; Biomonitoring sensor; Biotechnology; Bird; Birds; Block chain; Block diagram; Blog; Blogs; Blue force tracker network; Blue force tracking; Board combat systems; Board training systems; Boats; Booking system; Boosting; Border security; Both with; Bowman communications system; Bowman networks; Brain computer interfaces; Bridge system; Bridging; Broadband; Broadband communications; Broadband system; Broadcast system; Broadcasting; Browser; Bubbles; Building blocks; Bulk fuel delivery system; Business intelligence; Business process model; Business process protection; Buzz; Calibration; Camera display; Camera interface; Camera phone; Camera system; Cameras; Cameras sensors; Can be successful; Can bus; Capacitors; Capacity systems; Capture device; Cargo movement operations system; Cargo restraint rail systems; Cartographic engine; Cartography; Case management; Cast; Causeway system; Ccirm; Cctv infrastructure; Cell phone; Cell tower; Cells; Cellular; Cellular networks; Cellular phone; Cellular systems; Cellular technologies; Central processing unit; Centralized database; Cert; Cgis; Change detection; Chassis; Chemical tanker; Chip; Chips; Chipset; Cidne; Circuit; Cirt; Classifier; Client-server; Client computer; Client stations; Clip; Close circuit television system; Closed circuit television; Cloud; Cloud-based solutions; Cloud based services; Cloud computing; Cloud technologies; Cluster system; Clusters; Clutter; Cmos; Coalition shared database; Coalition shared database servers; Cockpit screens; Code technology; Code technology computer; Coding; Cognitive cyber physical systems; Cognitive radio; Cognitive radio network; Cognitive radio technology; Collaboration system; Collaborative combat technologies; Collaborative information technology; Collaborative network; Collect data; Collection coordination intelligence requirements management; Collection management; Collection system; Collectors; Combat cloud; Combat collaborative systems; Combat equipment; Combat information system; Combat management system; Combat net radio; Combat network; Combat system; Combined information data network exchange; Comfort sensor; Comint; Command and control module; Command automated information system; Command platforms; Command post of the future; Command teams system; Commercial aviation; Commercial off the shelf; Common analysis system; Common communication network; Common ground system; Common hardware systems; Common infrared countermeasure systems; Common inland transport system; Common operational picture; Common operational picture network; Communication and information systems security; Communication hub; Communication infrastructure; Communication machine; Communication media; Communication network; Communication network technology; Communication protocols; Communication satellite comsat technology; Communication technology; Communication tool; Communications channels; Communications computers; Communications device; Communications intelligence; Communications module; Communications systems; Community; Compact sensor; Compact system; Complex adaptive systems; Computational simulation; Computational systems; Computer; Computer-aided manufacturing; Computer-generated graphic; Computer algorithm; Computer and network intrusion detection systems; Computer graphics metafile technology; Computer graphics technology; Computer machine; Computer network; Computer operating systems; Computer program; Computer reference model technology; Computer science; Computer security; Computer simulation systems; Computer systems; Computers; Concept systems;

Configurable connectors; Configuration item system; Configuration management; Conflict management; Connect assault rifles; Connected binoculars; Connected devices; Connected weapons; Connectivity technologies; Connectors; Console; Constantly-updated common operational picture; Container asset management system; Container delivery system; Container ships; Content management; Context-aware computing; Control & reporting system; Control board; Control communications system; Control computer; Control research technology; Control system; Control unit; Controllers; Controlling devices; Converter; Convex hull; Cooling mechanism; Cooling system; Cooperation management information system; Cooperative fighting system; Copper network; Core network; Cormorant system; Cosmo-skymed system; Cots devices; Cots technologies; Cots technology; Countermeasure system; Counts machine; Cpof; Crawling; Cray-1; Cray xm-p-4; Crisis and emergency management; Crisis management organizations; Critical information systems; Cross-platform; Cryptanalysis; Crypto; Cryptographic equipment; Cryptography; Cryptologic system; Csd servers; Cueing system; Current sensors; Cutting-edge technology; Cyber-physical system; Cyber-technologies; Cyber-terrorism; Cyber battle management; Cyber command and control battle space management; Cyber defence; Cyber intelligence; Cyber security; Cyber security systems; Cyber warfare; Cybernetic control system; Cybernetics; Cybersecurity management system; Cyberspace; Cyclone; Daas; Darpa xg; Dashboard; Data-communications security; Data-intensive systems; Data-link module; Data-mining; Data-stream; Data-tracks-actions agent; Data-transmission; Data acquisition; Data analytics; Data bus; Data capture; Data collection; Data communications; Data container; Data curation; Data distribution; Data exchange; Data filtering; Data fusion; Data integration; Data interchange; Data link devices; Data link processor; Data link technology; Data loss protection; Data management; Data management system; Data modem; Data networks; Data preparation; Data processing network; Data processing systems; Data processing techniques; Data profiling; Data protection; Data representation; Data services; Data sharing; Data storage; Data transfer; Data visualization; Data warehousing; Database system; Databases; Datacenter; Ddos threat mitigation services; Debugging; Decision support; Decision support software; Decision support system; Decision support tools; Deepfakes; Defence acquisition system; Defence communication technology; Defence weapon systems; Defended network; Defense biometric identification system; Defense blood standard system; Defense communications system; Defense information network; Defense information systems; Defense information systems agency; Defense information systems network; Defense information technology; Defense intelligence information system; Defense logistics management system; Defense satellite communications system; Defense source registration system; Defense supply system; Defense support systems; Defense transportation system; Defense travel system; Degaussing; Deployable system; Derive; Desktop device; Detection radar systems; Detector system; Detectors; Detonation mechanisms; Devops methods; Dhcp server; Digital-tempo systems; Digital camera; Digital computer; Digital data links; Digital electro-optical systems; Digital information link technology; Digital map; Digital measurement system; Digital networks; Digital technology; Digital video manager; Diode; Directed-energy weapon; Directedenergy device; Disablement system; Discharge system; Discrete event system; Disparate information systems; Display; Display technologies; Disposal information management system; Disposal technology; Disruptive innovations; Disruptive technology; Dissemination of data; Dissemination systems; Distributed computing; Distributed databases; Distributed network; Distributed system; Distribution standard system; Distribution system; Dog mechanic; Down link; Download data; Drms; Drone; Drone systems; Dss software; Dual use technologies; Dust masks; Dynamic risk management; E-mail; E-mail system; E-verify; Earth observation; Earth observation space systems; Earth observation systems; Edge devices; Edge weapon system; Effectors; Eiffel; Electric furnace; Electrical systems; Electro-explosive devices; Electro-optical device; Electro-optical fire control system; Electro-optical sensor; Electro optical video; Electromagnetic emitters; Electromagnetic maneuver warfare; Electromagnetic modeling; Electromagnetic sensors; Electromechanical; Electronic communications systems; Electronic computing systems; Electronic counter; Electronic countermeasure sensors; Electronic countermeasures module; Electronic data interchange; Electronic device; Electronic document management; Electronic equipment; Electronic information system; Electronic sensors; Electronic support measure sensors; Electronic support systems; Electronic system; Electronic tracking system;

Electronic warfare; Electronic warfare management system; Electronic warfare sensors; Electronic warfare systems; Elint systems; Emac; Email server; Embedded systems; Emergency locator transmitter; Emergency position-indicating radio beacon; Emitters; Encapsulated system; Encyclopaedic database; End-to-end data management; Endeavors space; Energy device; Engine; Engineering systems; Entity resolution; Environmental health readiness system; Equipment discovery sensor; Equipment recognition semi-automatic tool; Erable system; Ergonomics; Esri arcsde; Essential emergency communications network; Ethernet; Evacuation system; Evaluation system; Event devices; Event management; Event management systems; Events emergencies system; Ew libraries management; Ew systems; Exact software; Exchange information; Execution system; Expert systems; Exploitation system; Explosive device; Explosive ordnance disposal technology; Extended-range guided munition; External networks; Extranet; Eye-safe laser rangefinder; Eye protection; Eye tracking; Facebook; Facial recognition software; Failure analysis; Falcon; Fault tolerance mechanisms; Faust systems; Fbis; Feathered flying machine; Federated database system; Feedback control systems; Feedback systems; Feeder systems; Félin infantry equipment system; Fertilizer; Fibers; Fibre network; Field artillery system; Fifth generation systems; Fighters battlefield management systems; Filaments; File transfer; File types; Filter systems; Filtering of data; Financial crimes enforcement network; Finite state machines; Fire control systems; Fire sensors; Fire support systems; Firefighting; Firewall; Firmware; First generation; Fishing boats; Fiss; Fits mission system; Fixed ground platform; Fixed sensors; Flailing mechanic; Flaps; Fleet operational command system; Flight simulation; Flir sensor; Focal; Force sensors; Form factor; Forward-looking infrared; Fourth generation; Frequency resource record system; Full-motion streaming video day and night; Full motion video; Full motion video modules; Full motion video sensors; Full spectrum cyber; Full spectrum targeting; Fusion analytics; Fusion information networks; Fusion mechanisms; Fusion module; Fusion sensor; Fusion system; Fuzzy logic; Gamss; Gate arrays; Gateway interfaces; Gateways; Gbit; Gdss; Gear; Genetic algorithms; Geo-localisation device; Geo-referenced common operational picture; Geo-referenced cop; Geo-referenced radar display; Geo referenced map; Geographic information system; Geolocalization technology; Geolocalized imaging; Geospatial analysis; Geospatial information systems; Geosuite; Geosynchronous systems; Gesture control; Gfe components; Gift; Gigaspace; Glasses; Global area reference system; Global automatic identification system; Global broadcast system; Global combat support system; Global command and control system; Global command support system; Global decision support system; Global information system; Global navigation satellite system; Global navigation systems; Global positioning systems; Global transportation network; Gloves; Gnss; Goggles; Google; Google cardboard; Google glass; Google vr sdk; Gorgon stare; Government furnished equipment components; Government off-the-shelf applications; Government off the shell; Gps navigation system; Gps receiver; Graphics system; Gripen; Grippers; Ground-air radio; Ground-based electronic warfare systems; Ground communications networks; Ground infrastructure networks; Ground network; Ground robot system; Ground sensors; Ground surveillance radars; Ground system; Ground ubiquitous surveillance system; Ground vehicles; Grounded theory; Groupware; Guidance module; Gun systems; Guns; Hacking; Hadoop; Hammers; Handheld devices; Hardware; Hardware systems; Harfang male system; Harvest; Head-up display; Headphones; Headset; Headset system; Health service support system; Heat sink; Heating system; Heavy-lift helicopter; Helicopter; Heterogeneous data sources; Hids; Hierarchical networks; Hierarchical wireless sensors; Hierarchical wireless sensors networks; High-frequency electronics; High-performance computing; High-power electronics; High-throughput; High bandwidth; High capacity data link; High data rate transmissions; High definition; High frequency system; High integrity telecoms system; Highly-sensitive electronics; Hits; Holographic; Homeland security; Homeland security information network; Hop communication system; Hose reel; Hosts; Hubs; Human-computer interaction; Human-computer interface; Human-machine system; Human intelligence; Human machine interface; Humanitarian logistics system; Hybrid cloud; Hydration; Hydration system; Hydrogel; Hypersonic weapons; Hypodermic needles; Ibm watson; Icts; Identification systems; Illustrative networks; Image analysis; Image analysis software; Image capture; Image capture devices; Image exploitation; Image management; Image processing systems; Imagers; Imagery intelligence analysis system; Imaging sensors; Imaging system; Imint sensors; Improvised

explosive devices; Incident command system; Inertial devices; Inertial navigation system; Inertial sensors; Infantry combat system; Influence diagrams; Information age networks; Information age technologies; Information and communication systems; Information architecture technology; Information assurance nonelectronic systems; Information battle system; Information data network; Information dissemination; Information electronic systems; Information exchange systems; Information feedback system; Information feedback system technology; Information fusion; Information into knowledge; Information management; Information networks; Information processing; Information security; Information security management system; Information sharing; Information system; Information systems security officer support; Information technology; Information technology computer; Information technology system; Information warfare; Infosec; Infrared; Infrared camera; Infrared camera system; Infrared image; Infrared sensor; Infrared system; Inland petroleum distribution system; Instagram; Integrated circuit; Integrated communications systems; Integrated computer aided manufacturing; Integrated operations and information system; Integrated platform management system; Integrated sensor commander shooter artillery; Integrated staff information system; Intel; Intelligence collection system; Intelligence data analysis; Intelligence data analysis system; Intelligence management cycle; Intelligence network; Intelligence signals; Intelligence surveillance and reconnaissance resources; Intelligence system; Intelligence technologies; Intelligent agent; Intelligent agents computer; Intelligent network management; Intelligent vehicles; Intelligent weapons; Inter-vehicle; Interaction networks; Interactive mapping interface; Interactive sensor; Interactive voice response; Intercom; Intercom system; Interconnected networks; Interconnects; Intercontinental ballistic missile systems; Interdependent networks; Interfaces; Interim polar system; International freight system; Internet; Internet of things; Internet protocol router network; Internet relay chat support; Internet technologies; Interoperable communications network; Intranet; Intransit visibility system; Intrusion detection; Intrusion detection systems; Inventory management system; Ionizing radiation; Ip routers; Isms; It service management; Itil; Jammers; Java; Javascript; Jc3iedm; Jdam-er; Jet propulsion; Jini; Joint command information systems; Joint communications network; Joint consultation, command, and control information exchange data model; Joint data network; Joint direct attack munition; Joint fires; Joint force communications system; Joint logistics system; Joint network management system; Joint operational command system; Joint precision airdrop system; Joint tactical radio system; Joystick control of camera; Json; Jsps; Julia; Kernel; Keyboard; Knowledge-based; Knowledge database; Knowledge management; Knowledge smart management software; Lan technology; Land battle management systems; Land battlespace systems; Land operations intelligence system; Landing rotor system; Language technology; Laptop; Laptop computer; Laptop devices; Large scale intelligent systems; Large scale software intensive system; Laser designator; Laser range finder devices; Laser rangefinder; Laser sight; Laser sight binoculars; Laser target designation system; Lasers; Layered system; Leaflet; Learning algorithms; Legacy systems; Legged robot; Lenses; Lethal autonomous devices; Liaison devices; Lidar; Light detection; Light drone; Lighter; Link 16 tactical data link; Linkedin; Linkpro; Linpack benchmark; Linux; Lithium polymer battery technology; Load sharing; Local area networks; Local sensor; Locator device; Logging; Logging systems; Logic devices; Logic network; Logistic system; Logistics network; Logistics software; Logistics support system; Long-term evolution; Long term evolution digital technologies; Low-power networks; Low altitude navigation & targeting infrared for night; Lte digital technologies; Lte networks; M-code; Machine-to-machine; Machine-to-machine links; Machine-to-machine systems; Machine learning; Machine translation; Magnetometer; Mainframe computer; Malware; Management information system; Management information technology; Management support systems; Management system; Manned aircraft; Manpower data center system; Mantadroid; Map-based query tools; Map-based visualization; Map display; Map reduce framework; Mapreduce; Maritime information management system; Maritime networks; Maritime security system; Maritime sensor; Maritime surveillance; Maritime surveillance system; Mass media; Massive computing systems; Material information resource system; Mccs; Mcop system; Measurement systems; Meat thermometer; Media technologies; Medical system; Merging sensor data; Mesh networked; Mesh networks; Message-handling systems; Messaging systems; Meta analysis; Meteorological sensors; Meteorological system; Meters; Micro air

vehicle; Microchips; Microsoft office; Microsoft office software; Microsoft outlook; Microsoft windows; Microwave; Middleware; Mil-std 2525 symbology; Mil2525c standard; Military 4g mobile networks; Military aircraft; Military communications systems; Military communications technology; Military computer; Military decision support systems; Military digital information network; Military earth observation system; Military electronic systems; Military global positioning system; Military grid reference system; Military information system; Military radio systems; Military space systems; Military space technologies; Military tactical networks; Military unmanned systems; Military weapon systems; Milsatcom system; Mini bird sized drones; Miniature sensors; Miniaturisation; Mirroring; Missile; Missile defense systems; Missile systems; Missile warning system; Mission command system; Mission management; Mixed reality systems; Mobile; Mobile ad hoc networks; Mobile airspace management system; Mobile cellular; Mobile communications technology; Mobile computing; Mobile data terminal; Mobile devices; Mobile network; Mobile networked workroom; Mobile phone; Mobile platform; Mobile processors; Mobile radio; Mobile technologies; Mobile technology; Mobile telephony; Mobile user objective system; Mobile weapon platform; Mobile wireless camera sensor; Mobility system; Modeling and simulation; Modeling tools; Modelling and simulation technologies; Modems; Monitor; Monitoring systems; Mortars; Motherboard; Motor; Motor vehicles; Mounted-dismounted reconnaissance, surveillance and target acquisition system; Moving target indicator; Multi-core computer; Multi-function radar systems; Multi-functional console; Multi-functions display; Multi-hypothesis track extraction from radar video; Multi-platform; Multi-role armoured vehicle; Multi-sensor correlator; Multi-sensor tracking; Multi-source system; Multi-spectral sensors; Multi-tactical data link network; Multi-target tracker; Multi-tiered isr systems; Multi-touch; Multi-touch screens; Multi sensor; Multi sensor vehicle; Multiband; Multicast; Multidomain system; Multifunctional information distribution system; Multihop; Multihop networks; Multihop wireless networks; Multilateration; Multimedia system; Multiple launch rocket system; Multiple network; Multiplexer; Myriad systems; Nanotechnology; Narrow band; Narrow band radio channels; Natural language processing; Naval combat management system; Naval combat systems; Naval communications networks; Naval electronic systems; Naval engagement systems; Naval radios; Naval surveillance systems; Navigation aids; Navigation module; Navigation systems; Navigational information system; Navy lighterage system; Navy surface gun systems; Near-infrared; Nearest-neighbor; Neighborhood; Net-centric electronic warfare; Nett warrior; Network; Network access control; Network centric warfare; Network data systems; Network infrastructure; Network intrusion detection systems; Network layer; Network management devices; Network management physical network; Network management system; Network planning; Network security; Network security devices; Networked image exploitation system; Networked sensors; Networked system; Networking devices; Networking systems; Networking technology; Networks; Neutralization systems; Next generation battle management systems; Ng bms; Night driving aiding system; Night vision binoculars; Night vision cameras; Noise filter; Nonorganic sensor; Northrop grumman information systems; Nosql; Notations; Nrbc detection sensors; Nuclear device; Nuclear explosive device; Object detection; Object management; Object orientation; Off-the-shelf offer; Off the shell; Office computer; Offshore bulk fuel system; Offshore petroleum discharge system; Olfactory sensors; On-board computing; On-screen control of camera; Onboard sensors; One-hop network; Open-source software; Open architecture; Open architecture intelligence; Open architecture systems; Open system; Open systems; Opengl; Operating systems; Operational communications network; Operational information systems; Operational picture; Operational system; Operator consoles; Optic; Optical fiber; Optical sensors; Optimal control systems; Optronic fire control sensor; Optronics sensors; Ordnance disposal publication system; Organic sensors; Orms; Orthogonal frequency division; Oscillators; Oth-t gold; Ounce sensor; Overhead sensor; Oxygen breathing apparatus; Ozone widget framework; Parallel computing; Parallel system; Paralysis; Pascal; Passive decoy systems; Passive network; Passive network monitoring; Passive solar heating system; Passwords; Patch management; Patrol boat; Pattern recognition; Perimeter detection sensors; Peripherals; Permanent control systems; Personal computers; Personal digital assistant; Personal protective equipment; Personal value systems; Petroleum distribution system; Phone; Phone computer; Photogrammetry; Physical data model system; Physical network; Physiographic; Ping; Pixel video sensors; Pixels; Planes; Planning system; Plant

control; Platform; Platform information technology; Platform management system; Plug; Plug-ins; Plug and play services; Plug and play systems; Plug systems; Pneumatic; Pointing device; Port analysis; Portable computer; Portable computer system; Portable operating system; Portable operating system interface; Portable surveillance radar system; Portable workstation; Posix; Power architectures; Power laser device; Power management; Power management module; Pre-tensioners; Precision-guided munitions; Precision attack systems; Precision level; Precision manufacturing; Precision targeting; Precision weapon; Predictive analysis; Preventive maintenance; Primary information technology; Principal component analysis; Printing; Private cloud computing; Probabilistic data association; Probes; Problem formulation; Processing data; Productions; Programming language; Project management software; Protection of data; Protection systems; Protective clothing; Protective system; Prototyping; Ptt headphone; Push to talk headphone; Qr codes; Quadcopters; Quantum; Quantum-safe cryptography; Quantum computers; Quantum computing; Quantum cryptography; Quantum technology; Radar; Radar control; Radar images; Radar sensor; Radar systems; Radar technology; Radiant system; Radio; Radio common hardware systems; Radio communications network; Radio connections; Radio devices; Radio direction finders; Radio frequency; Radio frequency identification; Radio headset; Radio link; Radio navigation system; Radio networks; Radio systems; Radio technology; Radiological dispersal device; Radiological exposure device; Radiotelephones; Railway network; Rangefinder; Raster; Re-transmission mechanism; Real-time analytics; Real-time common operating picture; Real-time communication; Real-time digital acquisition; Real-time sharing; Real-time systems; Real sharing information; Reaper system; Receivers; Recognition systems; Reconnaissance sensors; Reconnaissance systems; Reconnaissance technologies; Record analysis; Red force tracking; Reel system; Remote control; Remote control module; Remote deployment technology; Remote knowledge base; Remote optical video enhanced receiver; Remote sensing; Remotely piloted aircraft; Remotely piloted system; Remotely piloted vehicles; Repeater; Repeater system; Resistors; Resource management; Resources management module; Resources system; Retina; Retina detection sensors; Retrieval system; Rfi management; Rfid technology; Riot; Riots; Risk analysis; Risk assessment; Risk management; Risk management system; Rmon; Roaming; Robot; Robotic augmentation; Robotic systems; Robus tablet; Robust socio-technical networks; Rockets; Roip; Role-based access; Rotatable locator device; Rotatable pointing device; Rotor; Router; Routing; Routing protocols; Routing radio communication system; Rover terminal; Rq-4 global hawk uavs; Rs-232; Rugged tablet; Ruggedised laptop; Ruggedised tablet; Ruggedized workstation; Safety and security management; Safety harnesses; Satellite communications system; Satellite connections; Satellite photos; Satellite radio; Satellite systems; Satellite telephone; Satellite terminals; Satellites; Scada; Scada systems; Scaffolding; Scalable architecture; Scanner; Scooters; Scorpion combat information system; Scout robot; Scouting systems; Screens; Screwdrivers; Second generation; Secondary radar; Security information and event management; Security operations center support; Security systems; Security video; Seeker based weapon system; Selective service system; Self-diagnostics modules; Self-driving vehicle; Self-healing modules; Semantic mapping; Semantic search; Semantic search engine; Semi-autonomous battlefield systems; Sensor; Sensor data fusion; Sensor fly; Sensor integration system; Sensor modeling; Sensor networks; Sensor platform; Sensor system; Sensors; Sensors alert system; Sentiment analysis; Server; Service-oriented architecture; Service deployment systems; Service discovery; Servlets; Share information; Sharing tactical information; Shas; Shazam; Ship; Ship navigation sensors; Ships; Sigfox; Sigint; Signal-noise ratio; Signal processing; Signals intelligence processing; Simulation; Simulation-based evaluation tools; Simulation software; Simulation systems; Simulation technologies; Simulators devices; Simultaneous management; Simultaneous multiple sensor; Sincgars; Sincgars system; Single channel radio; Single platform; Single virtual network; Slides; Small world network; Smart-map elements; Smart and cognitive systems; Smart card; Smart grid; Smart machines; Smart support; Smart systems; Smartphone; Snapshot; Sniper detection sensors; Social media; Social media network; Social network; Sociotechnical; Sockets; Software; Software-defined radio; Software engineering services; Software infrastructure; Software radio technology; Soldier radio waveform; Soldiers planning logistic; Sonar; Sonar systems; Space sigint systems; Space surveillance systems; Space system; Spark; Species; Spectrum management; Spectrum sensing; Speech recognition; Speech technology;

Speed sensor; Spit; Spreadsheet application; Spreadsheets; Sprinklers; Staff information system; Standard pc hardware; Statistical analysis; Statistical methods; Stem; Stemming; Still images; Storage server; Storage system; Stovepipe systems; Strategic planning system; Stream processing; Strobes; Strong artificial intelligence; Structured analysis; Submarine; Submarine technology; Subsurface sensor; Subsurface systems; Subsystems management interfaces; Subversion; Suite b; Supercomputer; Surface sensor; Surface to air missile interface; Surveillance camera; Surveillance radar station technology; Surveillance sensors; Surveillance systems; Surveillance technologies; Swarm computing; Switchboards; Switches; Synthetic aperture radar; Synthetic biology; System analysis; System architecture design; System configuration; System core; System design; System dynamics; System integrator; System of marks; System of systems; System testing; T-test; Tablet; Tablet computer; Tac automated manifesting system; Tactical air control system; Tactical airspace integration system; Tactical area networks; Tactical communication system; Tactical computers; Tactical data link; Tactical data link network; Tactical data link sensors; Tactical data link system; Tactical electronic warfare system; Tactical ground reporting system; Tactical information management; Tactical information systems; Tactical local area system; Tactical module; Tactical reconnaissance radars; Tactical trunk network; Tactical water distribution system; Tacticos combat management system; Tactile watches; Tagging; Tailoring technology; Tandem; Tank; Tankers; Tanks; Target acquisition; Target acquisition system; Target attack radar system; Target locating systems; Target recognition; Target snapshots; Target system; Targeting module; Targeting tool; Technical surveillance technologies; Telecom operators; Telecommunications control technology; Telecommunications networks; Telecommunications systems; Telecommunications technologies; Telecoms; Telegraph; Telemedicine; Telephone; Telephone circuit; Telephone system; Telepresence; Telepresence systems; Television; Temperature sensor; Term computer; Terrain avoidance system; Terrain contour matching; Terrestrial communications; Terrestrial communications system; Testbed; Text analysis; Text management; Theater air control system; Theater air ground system; Theater distribution system; Thermal cameras; Thermal imager; Thermal imaging cameras; Thermal imaging device; Thermal imaging sensor; Thermometer; Thermostat; Threat management system; Threat modeling; Throttle; Tie down; Tigr; Time sensitive targeting; Time sensor; Timing device; Total data quality management; Total exposure health sensor; Touch navigation; Touchscreen; Track management; Trackball; Tracked vehicles; Tracker; Tracking radar; Tracking systems; Tracks; Tracks container; Traffic control; Traffic shaping; Training system; Transceiver; Transistors; Transmission media; Transmission technology; Transmitters; Transponders; Transport mechanism; Transport systems; Transportation system; Traps; Trend analysis; Triple play; Trucks; Trunking; Trusted computing; Tunneling; Tuple-space; Tv camera; Twitter; Two-way communication; Ultra-wideband; Ultraviolet radiation; Umts; Unattended ground sensor; Unattended sensor; Underwater acoustic sensors; Underwater systems; Unicast; Unified modeling language; Unify model language; Universal mobile telecommunications system; Unmanned aerial reconnaissance systems; Unmanned aerial system; Unmanned aerial vehicles; Unmanned aircraft; Unmanned aircraft system; Unmanned autonomous systems; Unmanned maritime systems; Unmanned systems; Unmanned vehicles; Unmanned weapons systems; Up link; User interface; User interface module; Vacuum tubes; Variable message format protocol; Vcbi armored infantry fighting vehicle; Vehicle mission systems; Vehicle system; Vehicles; Velocity container delivery system; Vessel; Video-conferencing; Video cameras; Video capture devices; Video exchanges; Video games; Video management; Video sensors; Video server; Video streaming; Video technologies; Video teleconferencing; Virtual environment; Virtual intelligence repository; Virtual reality; Virtualization; Vision device; Vision sensors; Visual augmentation systems; Visual computing; Vmf on demand; Voice-over-radio; Voice over ip; Voice radio circuit; Voice technology; Voip; Voip technology; Warfighting; Warning search radar; Warning system; Water combat systems; Water levels; Water purification unit; Waterway system; Waveforms; Waveguide; Wavelengths; Weapon; Weapon control systems; Weapons machines; Weapons sensors; Weapons systems; Wearable computer; Wearable computing; Wearable display; Weather radar; Weather sensor; Web-based system; Web application; Web based delivery; Web browser; Web mapping; Web pages; Web services; Web site; Welders; Whiteboards; Wi-fi; Wide area network; Wideband gapfiller satellite system; Wideband global satcom system; Wideband network; Wifi;

Winbms; Wind tunnels; Window management; Window system; Windows; Wireless; Wireless communication; Wireless communication system; Wireless communications technology; Wireless devices; Wireless lan; Wireless mesh networks; Wireless multimedia networks; Wireless network; Wireless sensor; Wireless sensor network; Wireless technology; Wolframalpha; Work light; Workforce management; Workforce management software; Workstations; World geodetic system; World wide web; Worldwide intelligence communications system; Youtube; Zigbee® network; Zoom.

Appendix 7. Results of the relevance matrix – UNIPI and UNIBX team

This appendix contains additional visualization of the relevance matrix obtained by UNIPI and UNIBX team for the exploration of the relationships between applications and technologies related to the C4ISTAR domain, as presented in Paragraph 4.2.3 “Relevance matrix: C4ISTAR domain”.

With the purpose to give a look on the intensity of each pair relevance, the relevance matrix is visualized using a heatmap reported in Figure 8 where the scores contained in the matrix are represented as colors.

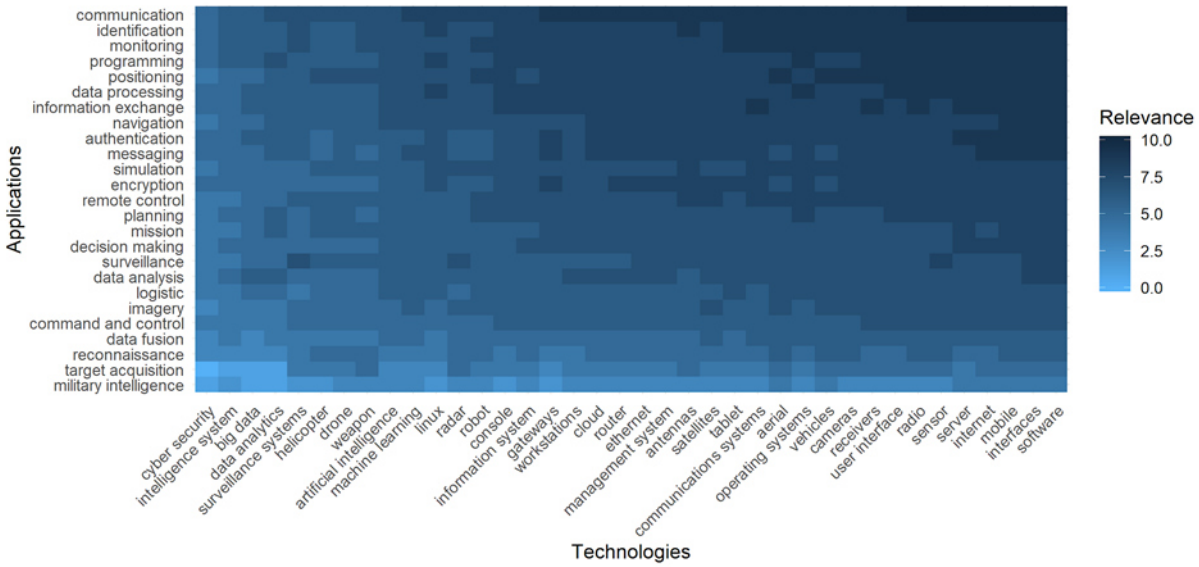


Figure 8 - Heatmap of Relevance matrix.

Moreover, the results obtained in the relevance matrix can be visualised in a network, as shown in Figure 9, where:

- each node of the graph corresponds to an application or a technology;
- an edge connects each pair technology-application in the C4ISTAR domain;
- the size of the nodes is proportional to the total number of the in-degree and out-degree, that is the number of edges that are incident to each vertex; a node with more connections has a larger diameter, so this metric indicates which technologies/applications are more connected to the others;
- the thickness of the edges is proportional to the relevance value of each pair technology-application, based on the relevance matrix, in particular only the edges with a relevance greater than 7 have been reported;
- the distribution and the colours of the nodes is based on the modularity of the network ; it indicates the density of connections among nodes and allows to detect community structures in the network [90], in fact networks with high modularity have dense connections among nodes within modules but sparse connections among nodes in different ones; modularity ranges between [-½; 1]. In the network of Figure k modularity is equal to 0.185.

In this way it is possible to have a complete vision of the emerging technologies and related applications in C4ISTAR domain and identify possible paths for educational programmes.

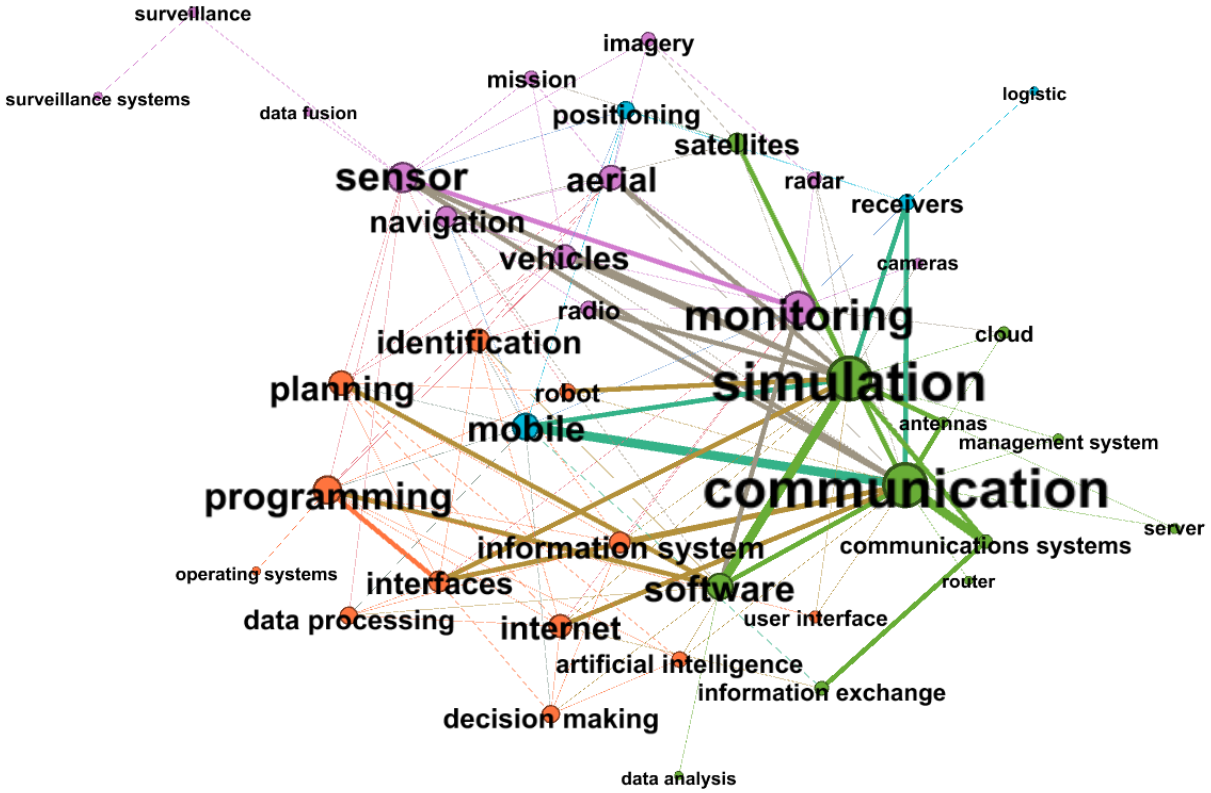


Figure 9 - Network of technologies and applications in C4ISTAR domain.

Appendix 8. UC3M & UNISEVILLE Industrial Survey

This appendix contains the industrial survey conducted by UC3M and UNISEVILLE team.

Survey

ASSETS+ European Project. Cybersecurity in the Defence sector. Technology mapping

This questionnaire is intended to gather your perspectives on the current and envisioned status of different cybersecurity technologies that are or can be applied in the defence sector.

This work is part of the ASSETS+ (Alliance for Strategic Skills addressing Emerging Technologies in Defence) European project. The results of this survey will inspire the future creation of teaching, training and upskilling initiatives for cybersecurity in defence.

No personal information is collected in this questionnaire. Moreover, results and opinions will be aggregated and will not be published individually.

This form contains 5 questions displayed in 3 pages and it will only take you around 10 minutes. We very much appreciate your assistance.

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

ASSETS+ European Project. Cybersecurity in the Defence sector. Technology mapping

* Required

Company profile

Company name *

.

Country *

.

Back Next

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

Current cybersecurity technologies in the defence sector

This question focuses on the current status of cybersecurity technologies and their application to the defence sector. In this regard, we need to assess their current maturity and relevance.

Please rate the MATURITY IN YOUR COMPANY of the following cybersecurity technologies. In this context, maturity refers to the degree to which each technology is applied in your institution. Leave it blank if the technology is unknown for you.

	Low	Medium	High
Identification & Authentication	○	○	○
Authorization & Access Control	○	○	○
Firewalls	○	○	○
Cyber range (cybersecurity training)	○	○	○

Please rate the RELEVANCE IN THE DEFENSE SECTOR (DEF) and IN YOUR COMPANY (COM) of the following cybersecurity technologies. In this context, relevance refers to the degree to which each technology is regarded as necessary. Leave it blank if the technology is unknown for you

	Low (COM)	Medium (COM)	High (COM)	Low (DEF)	Medium (DEF)	High (DEF)
Identification & Authentication	☐	☐	☐	☐	☐	☐
Authorization & Access Control	☐	☐	☐	☐	☐	☐
Firewalls	☐	☐	☐	☐	☐	☐
Cyber range (cybersecurity training)	☐	☐	☐	☐	☐	☐
Encryption	☐	☐	☐	☐	☐	☐
Certification	☐	☐	☐	☐	☐	☐
Endpoint Security	☐	☐	☐	☐	☐	☐
Mobile & IoT Security	☐	☐	☐	☐	☐	☐

Cybersecurity technologies and their application in the defense sector

Please, specify up to 5 DEFENSE APPLICATIONS of cybersecurity technologies.

Your answer

Please, specify up to 5 cybersecurity TECHNOLOGIES that could be relevant in the near future IN THE DEFENSE SECTOR and that they were not previously mentioned.

Your answer

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

Skills readiness in the defence sector

This section focuses on the available HUMAN RESOURCES in the labor market.

FROM YOUR COMPANY VIEWPOINT, please rate the availability of skilled professionals in the labor market for each cybersecurity technology. Use "low" if it is very hard to find a suitable candidate, "medium" if it is possible to find one with moderate effort and "high" if it is very easy to find good candidates for that technology. Leave it blank if the technology is unknown for you.

	Low	Medium	High
Identification & Authentication	○	○	○
Authorization & Access Control	○	○	○
Firewalls	○	○	○
Cyber range (cybersecurity training)	○	○	○
Encryption	○	○	○
Certification	○	○	○

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

Survey responses

# Comp.	Country	Please, specify up to 5 DEFENSE APPLICATIONS of cybersecurity technologies.	Please, specify up to 5 cybersecurity TECHNOLOGIES that could be relevant in the near future IN THE DEFENSE SECTOR and that they were not previously mentioned.
1	Spain	Proofpoint, Sophos, Retarus, Beyond Trust, One Identity	
2	Spain	Physical security, firewalls, antimalware, access control	Advanced identification, AI security analysis, ciphering
3	Spain		
4	Spain	Acquisition of Cyber Situational Awareness, Support to decision-making in military operations on the cyberspace (C2), Education and Training (Cyber Range), Information sharing and distributed Common Operational Picture (COP), Cross-domain Intelligence, Surveillance, Target Acquisition, Reconnaissance (ISTAR), Punishment and Joint Fires (Active Cyber Defence)	Dual-use and unified Cyber Threat Intelligent management, Prediction/Anticipation of multi-step attacks, End-to-End trust on IoT/edge/5G environments, Model and Simulation of neutral and adversarial activities on the cyberspace, Convergence cybersecurity + Electronic Warfare (OSI Layer 1 up to Layer 3)
5	Spain	Drones protection, geopositioning spoofing protection, mission logs protection, mission communications and IA protection, IA applied to foreseen conflicts	GNSS, IA, DDS, TTEthernet, VoIP

	TECHONOLOGIES																							
# Comp.	1	2	3	4	5	6	7	8	9	10	11	12	13	14	15	16	17	18	19	20	21	22	23	24
	Please rate the MATURITY IN YOUR COMPANY of the folloing cybersecurity technologies. In this context, maturity refers to the degree to which each technology is applied in your institution. Leave it blank if the technology is unknown for you.																							
1	3	3	3	3	2	2	3	3	3	3	3	3	3	3	3	3	3	3	2	3	3	3	2	3
2	2	1	3	2	2	3	1	1	1	1	3	3	2	1	1	1	1	3	3	1	2	2	1	1
3	1	2	1	2	3	3	1	3	2	2	2	2	2	1	1	1	2	2	3	2	2	2	1	2
4	3	3	3	3	3	3	3	2	2	2	2	3	2	2	2	2	3	3	3	3	2	3	3	2
5	3	3	3	2	3	3	3	2	2	2	3	3	2	2	1	2	2	2	2	2	2	2	2	2
	FROM YOUR COMPANY VIEWPOINT, please rate the availability of skilled professionals in the labor market for each cybersecurity technology. Use "1" if it is very hard to find a suitable candidate, "2" if it is possible to find one with moderate effort and "3" if it is very easy to find good candidates for that technology. Leave it blank if the																							
1	2	2	3	2	2	1	2	3	3	1	1	2	2	1	1	2	2	2	2	1	1	1	1	1
2	1	1	3	3	1	2	3	3	2	2	1	3	2	2	2	1	1	3	2	1	3	2	2	1
3	2	2	2	2	2	2	2	2	2	2	3	2	1	1	1	2	3	3	2	2	2	2	2	2
4	1	1	2	1	1	2	2	2	2	2	2	1	2	2	2	2	2	2	2	2	2	2	1	1
5	2	2	3	1	2	1	2	2	1	1	2	1	2	1	1	1	1	2	1	1	2	1	1	1
	Please rate the RELEVANCE IN THE DEFENSE SECTOR (DEF) and IN YOUR COMPANY (COM) of the folloing cybersecurity technologies. In this context, relevance refers to the degree to which each technology is regarded as necessary. Leave it blank if the technology is unknown for you																							
1	3 (DEF)	3 (DEF)	3 (DEF)	2 (DEF)	2 (DEF)	2 (DEF)	3 (DEF)	3 (DEF)	3 (DEF)	3 (DEF)	3 (DEF)	3 (DEF)	3 (DEF)	3 (DEF)	3 (DEF)	3 (DEF)	3 (DEF)	2 (DEF)	2 (DEF)	3 (DEF)	3 (DEF)	3 (DEF)	3 (DEF)	3 (DEF)
2	2 (COM), 3 (DEF)	2 (COM), 3 (DEF)	2 (COM), 3 (DEF)	3 (COM), 3 (DEF)	3 (COM), 3 (DEF)	3 (COM), 2 (DEF)	3 (COM), 3 (DEF)	3 (COM), 2 (DEF)	1 (COM), 1 (DEF)	2 (COM), 3 (DEF)	1 (COM), 2 (DEF)	2 (COM), 3 (DEF)	3 (COM), 3 (DEF)	2 (COM), 3 (DEF)	1 (COM), 1 (DEF)	2 (COM), 3 (DEF)	2 (COM), 3 (DEF)	3 (COM), 3 (DEF)	3 (COM), 2 (DEF)	1 (COM), 2 (DEF)	2 (COM), 3 (DEF)	2 (COM), 3 (DEF)	1 (COM), 3 (DEF)	2 (COM), 2 (DEF)
3	1 (COM)	1 (COM)	2 (COM)	2 (COM)	2 (DEF)	2 (DEF)		3 (COM), 3 (DEF)	1 (COM)	2 (COM)	2 (COM)	2 (COM), 2 (DEF)	1 (COM)				2 (COM)	2 (COM), 2 (DEF)	2 (COM), 2 (DEF)	2 (COM)	2 (COM)			
4	3 (COM), 3 (DEF)	3 (COM), 3 (DEF)	3 (COM), 3 (DEF)	3 (COM), 3 (DEF)	3 (COM), 3 (DEF)	3 (COM), 3 (DEF)	2 (COM), 2 (DEF)	2 (COM), 2 (DEF)	2 (COM), 2 (DEF)	2 (COM), 3 (DEF)	1 (COM), 1 (DEF)	2 (COM), 3 (DEF)	1 (COM), 2 (DEF)	3 (COM), 3 (DEF)	1 (COM), 1 (DEF)	2 (COM), 2 (DEF)	3 (COM), 3 (DEF)	3 (COM), 3 (DEF)	3 (COM), 3 (DEF)	2 (COM), 3 (DEF)	1 (COM), 2 (DEF)	3 (COM), 3 (DEF)	3 (COM), 3 (DEF)	1 (COM), 1 (DEF)
5	3 (COM), 3 (DEF)	3 (COM), 3 (DEF)	3 (COM), 3 (DEF)	3 (COM), 3 (DEF)	3 (COM), 3 (DEF)	3 (COM), 3 (DEF)	3 (COM), 2 (DEF)	3 (COM), 2 (DEF)	1 (COM), 2 (DEF)	3 (COM), 3 (DEF)	2 (COM), 3 (DEF)	3 (COM), 2 (DEF)	3 (COM), 3 (DEF)	3 (COM), 3 (DEF)	2 (COM), 2 (DEF)	3 (COM), 3 (DEF)	3 (COM), 3 (DEF)	3 (COM), 2 (DEF)	3 (COM), 3 (DEF)	3 (COM), 2 (DEF)	3 (COM), 2 (DEF)	3 (COM), 3 (DEF)	3 (COM), 2 (DEF)	3 (COM), 3 (DEF)

Appendix 9. Technologies description – UC3M and UNISEVILLE team

This appendix, in Table 9, lists the technologies identified by UC3M and UNISEVILLE team for the Cybersecurity domain.

Purpose		#	Technology	Description
Defensive	Protect	1	Identification & Authentication	Provision of assurance that a claimed characteristic of an entity is correct [74]
		2	Authorization & Access Control	The granting of rights, which includes the granting of access based on access rights. [75]
		3	Firewalls	Set of techniques to actively protect a network, such as firewalls, DDoS protections
		4	Cyber range	A designated set of assets and capabilities which can be integrated at the appropriate classification levels and controls to conduct research, development, demonstration, testing, or evaluation of military capabilities supported in, through, and from cyberspace, or to train military personnel in conducting cyber operations [76]
		5	Encryption	Encipherment of data within or at the source end system, with the corresponding decipherment occurring only within or at the destination end system. [77]
		6	Certification	Processes to attest the identity or an attribute of a system or service
		7	Endpoint Security	Endpoint security systems protect computers and other devices on a network or in the cloud from cybersecurity threats. Endpoint security has evolved from traditional antivirus software to providing comprehensive protection from sophisticated malware and evolving zero-day threats. [78]
		8	Mobile & IoT Security	Set of techniques to protect resource-constrained devices
		9	Cloud and virtualization security	Set of technologies related to protect cloud-based or virtualized environments.
		10	Vulnerability management	The process of identifying, assessing and correcting vulnerabilities, defined as "Weakness in an information system, system security procedures, internal controls, or implementation that could be exploited or triggered by a threat source" [79]
		11	Malware analysis	Acquiring sensitive data by disassembling and analyzing the design of a system component. [80]
		12	Hardware security	Set of physical protections applied to ensure the correct execution and functioning of a device
	Detect	13	Intrusion Prevention/Detection Systems (IDS/IPS)	Hardware or software products that gather and analyze information from various areas within a computer or a network to identify possible security breaches, which include both intrusions (attacks from outside the organizations) and misuse (attacks from with the organizations). [81]

Purpose		#	Technology	Description
		14	Cyber threat Intelligence	Activities using all "intelligence" sources in support of Cyber Security to map out the general cyber threat, to collect cyber intentions and possibilities of potential adversaries, to analyse and communicate, and to identify, locate, and allocate the source of cyber-attacks. [82]
		15	Honeypots	A system (e.g., a web server) or system resource (e.g., a file on a server) that is designed to be attractive to potential crackers and intruders, like honey is attractive to bears. [83]
		16	Security Operations	Set of technologies available in a Security Operations Center, which according to McAfee, it "is a centralized function within an organization employing people, processes, and technology to continuously monitor and improve an organization's security posture while preventing, detecting, analyzing, and responding to cybersecurity incidents." [84]
	Identify	17	Risk assessment & management	The process of identifying, assessing, and responding to risk. [85]
		18	Compliance and assurance	Adherence to, and the ability to demonstrate adherence to, mandated requirements defined by laws and regulations, as well as voluntary requirements resulting from contractual obligations and internal policies [86]
		19	Secure software development	Software development process which considers all security-related issues from the very first step.
	Respond	20	Forensic analysis	The practice of gathering, retaining, and analyzing computer-related data for investigative purposes in a manner that maintains the integrity of the data. [87]
		21	DoS Protection	Implementations to protect against the existence of denial of service attacks.
	Recover	22	Cyber resilience	The process to ensure that recovery of operations will be assured should any unexpected or unwanted incident occur that is capable of negatively impacting the continuity of essential business functions and supporting elements. [88]
Offensive		23	Open Source Intelligence (OSINT)/ Private Intelligence (PRIVINT)	Intelligence from publicly/ privately available information that is collected exploited and reported to address a specific intelligence requirement. [89]
		24	Penetration Testing / Red Teaming	Set of tools and techniques focused on attacking a device, service or host to identify weaknesses for later protection

Table 9 - The technologies identified in the Cybersecurity domain.

Appendix 10. Results of the relevance matrix– UC3M and UNISEVILLE team

This appendix shows the Relevance matrix of the Cybersecurity applications and technologies, compiled based on the expert judgment. The results are shown in Figure 10 by using the relevance score and a colour scale: from 0 and red, meaning no relevant, to 10 and green, meaning high relevant.

		Technologies																						
		Identification & Authentication	Authorization & Access Control	Firewalls	Cyber range	Encryption	Certification	Endpoint Security	Mobile & IoT Security	Cloud and virtualization security	Vulnerability management	Malware analysis	Hardware security	Intrusion Prevention/Detection Systems (IDS/IPS)	Cyber threat Intelligence	Honeypots	Security Operations	Risk assessment & management	Compliance and assurance	Secure software development	Forensic analysis	DoS Protection	Cyber resilience	Open Source Intelligence (OSINT)/ Private Intelligence (PRMNT)	Penetration Testing / Red Teaming
Defense applications	Defense industrial base collaboration	7	9	10	0	9	9	10	3	3	10	7	9	9	9	0	9	10	10	8	8	9	7	7	9
	Cyber security awareness and training	2	3	3	10	1	1	1	3	2	1	3	3	2	6	0	3	3	3	1	3	3	3	8	10
	Operations Security (OPSEC)	7	10	9	9	9	8	9	7	7	9	7	9	9	6	7	10	9	7	7	3	9	9	6	3
	Cyber Operations (CO)	7	9	9	9	8	3	8	8	6	9	7	3	8	7	7	7	8	2	2	9	7	7	10	10
	Military Information Support Operations (MISO)	7	9	1	1	6	2	3	2	3	2	0	3	3	7	0	6	2	3	2	1	3	10	8	3
	Command and Control Support	8	9	3	3	6	3	3	2	3	2	0	3	2	7	0	8	2	3	2	1	3	10	8	3
	Secure Communications (COMSEC)	8	10	9	0	10	9	7	0	0	0	0	0	8	0	0	7	0	9	0	0	10	6	0	0
	Cyber electronic warfare activities (CEWA)	7	8	8	8	7	7	7	3	2	6	3	10	8	10	3	7	8	7	9	3	10	10	3	10

Figure 10 - Relevance matrix of the cybersecurity domain.

References

[1] Belin J., Guille M., Lazaric N. and Mérindol V. (2018). Defence Firms Adapting to Major Changes in the French R&D Funding System. Defence and Peace Economics.

[2] NIST 800-171v2. Available at: https://csrc.nist.gov/publications/detail/sp/800-171/rev-2/final

[3] Rivera, R. et al (2017), Achieving a sovereign and trustworthy ICT industry in the EU, https://www.europarl.europa.eu/RegData/etudes/STUD/2017/614531/EPRS_STU(2017)614531_EN.pdf, last access May 2021

[4] Report: Cybersecurity Technologies & Market - Focus on Europe - 2017-2022. Available at: https://homelandsecurityresearch.com

[5] Momentum Cyberscape 2019 . Available at https://momentumcyber.com/docs/CYBERscape.pdf

[6] CSF (NIST): "Framework for Improving Critical Infrastructure Cybersecurity". Available at: https://www.nist.gov/cyberframework

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

[8] Secure Controls Framework (SCF). Available at: https://www.securecontrolsframework.com

[9] Topics from MILCOM2018, and sessions and papers accepted at MILCOM2019. Available at: https://events.afcea.org/MILCOM19/Public/enter.aspx

[10] Cybersecurity Trends for 2018, Westchester County Business Journal, May 28, 2018, Vol.54 (22), p.10

[11] U.S. Cyber Command Technical Challenge Problems Guidance & papers. Available at: https://www.cybercom.mil/Portals/56/Documents/Technical%20Outreach/Technical%20Challenge%20Problems.pdf?ver=2019-07-02-151118-497

[12] Oksanen, Kaisa, Mikko Dufva, and Toni Ahlqvist. "Anticipating the Emerging Innovation Ecosystem of Synthetic Biology." ISPIM Conference Proceedings. The International Society for Professional Innovation Management (ISPIM), 2015.

[13] Baldassarre, Maria Teresa, et al. "Cloud computing for education: A systematic mapping study." IEEE Transactions on Education 61.3 (2018): 234-244.

[14] Chiarello F., Trivelli L., Bonaccorsi A., Fantoni, G. (2018). Extracting and mapping industry 4.0 technologies using Wikipedia. Computers in Industry, 100, 244-257

[15] Giordano V., Cervelli E., Chiarello F. (2019). Defining definition: A Text mining Approach to Define Innovative Technological Fields, special track on Data science for innovation. R&D Management Conference, Paris, 17-21 June 2019

[16] L. Boytsov (2011). Indexing methods for approximate dictionary searching: comparative analyses. ACM Journal of experimental algorithmics 16 1-88. G. Navarro (2001). A guided tour to approximate string matching. ACM Computing Surveys 33 31-88

[17] 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.

[18] 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.

[19] 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.

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

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

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

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

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

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

[26] 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.

[27] 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.

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

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

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

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

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

[33] 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.

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

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

[36] 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.

[37] 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.

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

[39] 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.

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

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

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

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

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

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

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

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

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

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

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

[51] 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.

[52] 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.

[53] 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.

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

[55] 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).

[56] 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.

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

[58] 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

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

[60] 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).

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

[62] 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

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

[64] 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.

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

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

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

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

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

[70] 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.

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

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

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

[74] ISO/IEC. (2014). ISO/IEC 27000: 2014 (E) Information technology—Security techniques—Information security management systems—Overview and vocabulary.

[75] Reihe, I. S. O. (1989). IEC 7498 ISO/IEC 7498-1: 1994-11. Information technology–Open Systems Interconnection–Basic Reference Model: The Basic Model ISO, 7498-2.

[76] Damodaran, S. K., & Smith, K. (2015). CRIS Cyber Range Lexicon, Version 1.0 (No. MIT-LL-59-0001). MASSACHUSETTS INST OF TECH LEXINGTON LINCOLN LAB

[77] ISO 7498-2:1989. Information processing systems — Open Systems Interconnection — Basic Reference Model

[78] McAffee, https://www.mcafee.com/enterprise/es-es/security-awareness/endpoint.html

[79] NIST, S. (2013). 800-53: 2013. Security and Privacy Controls for Federal Information Systems and Organizations.

[80] Glossary of Terms, SANS. https://www.sans.org/security-resources/glossary-of-terms/

[81] Assurance, I. National Information Assurance. (IA) glossary. Tech. Rep. 4009, 2010. Online Available: https://www.dni.gov/files/NCSC/documents/nittf/CNSSI-4009_National_Information_Assurance.pdf

[82] NATO - Cyber Security Strategy for Defence, ACST Strategy-CyberSecurity-001, 2014

[83] National Information Assurance (IA) glossary. Committee on National Security Systems. CNSS instruction no.4009.april 2010.

[84] "What Is a Security Operations Center (SOC)?". McAfee. https://www.mcafee.com/enterprise/es-es/security-awareness/operations/what-is-soc.html

[85] Framework for Improving Critical Infrastructure Cybersecurity, NIST 2014

[86] ISACA, Cybersecurity Glossary, 2014. https://www.isaca.org/resources/glossary

[87] NIST, S. (2004). 800-61. Computer security incident handling guide, 800-61.

[88] ISO-18028-1:2006. Information technology — Security techniques — IT network security

[89] Josh Huff, SANS Security Summit 2018, https://www.sans.org/cyber-security-summit/archives/file/summit-archive-1533737204.pdf

[90] Vincent D Blondel, Jean-Loup Guillaume, Renaud Lambiotte, Etienne Lefebvre, Fast unfolding of communities in large networks, in Journal of Statistical Mechanics: Theory and Experiment 2008 (10), P1000

[91] Mitre ATT&CK attacks matrix. Available at: https://attack.mitre.org

[92] CyberOpsCertificate Curriculum. University Carnegie Mellon. Available at: https://www.cmu.edu/ini/academics/cyberops.html

[93] ECSO cybersecurity market radar. Available at: https://www.ecs-org.eu/documents/uploads/the-ecso-cybersecurity-market-radar-high-resolution.pdf

[94] No. 1 Cyber Warfare for JAs. Dickerson, Phillip ; Berger, Joseph. The Army Lawyer, Nov/Dec 2018, pp.40-45

[95] European Cybersecurity Centres of Expertise Map - Definitions and Taxonomy. Joint Research Centre (JRC). ec.europa.eu/jrc/en/publication/european-cybersecurity-centres-expertise-map-definitions-and-taxonomy , last access April 2021

[96] ENISA(2021), available at: https://www.enisa.europa.eu/news/enisa-news/exploring-research-directions-in-cybersecurity, last access May 2021

[97] ENISA (2021), Cybersecurity research directions for the EU's Digital Strategic Autonomy, https://www.enisa.europa.eu/publications/cybersecurity-research-directions-for-the-eu2019s-digital-strategic-autonomy/, last access May 2021