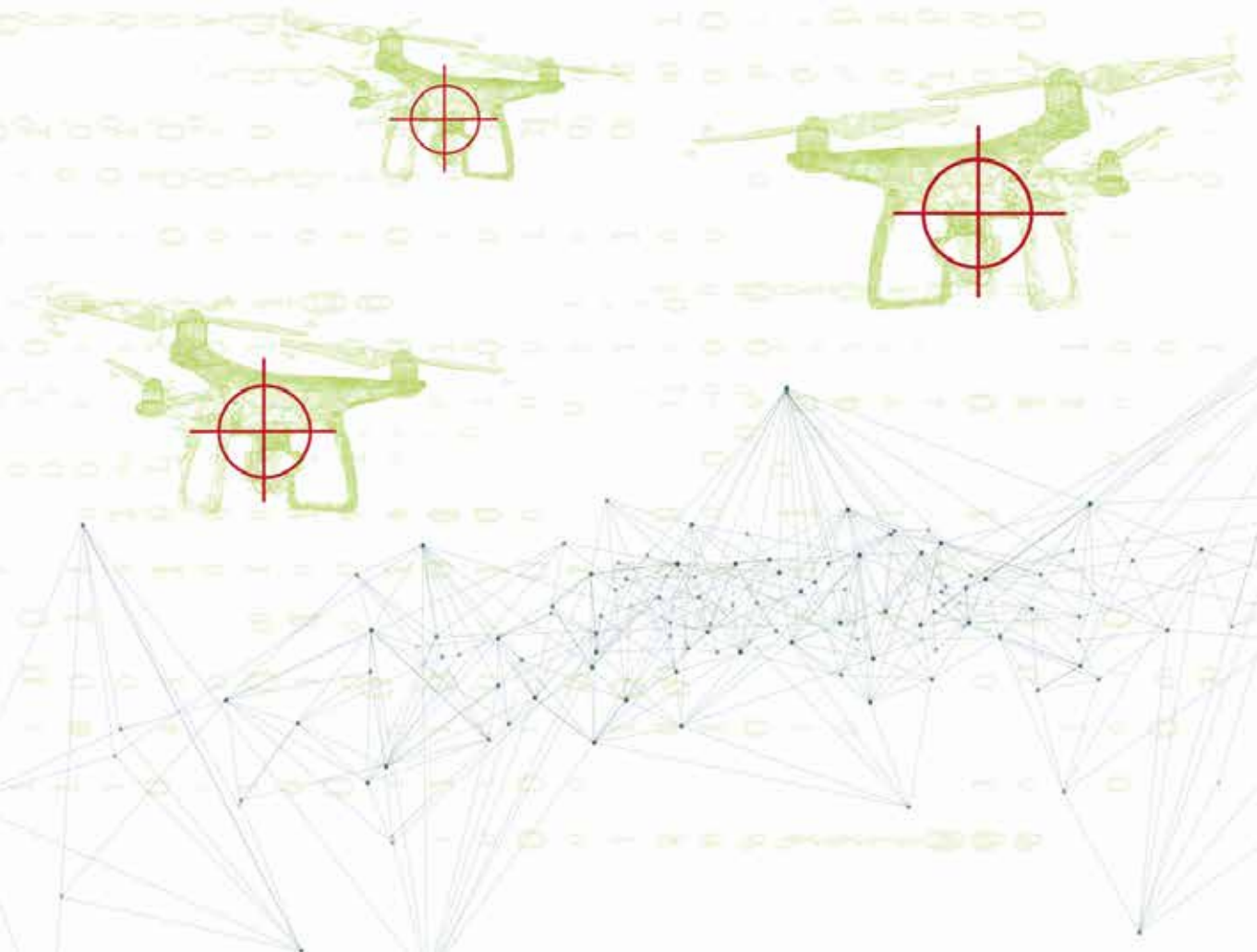
Foro Empresas Innovadoras

amper

SITUATION AND TRENDS IN THE USE OF ARTIFICIAL INTELLIGENCE IN THE DEFENCE SECTOR



Imprime: Estrella Servicios Gráficos, S. L.
28991 Torrejon de la Calzada (Madrid).

ISBN: 978-84-09-75701-5

Abridged version of the final report[01]

Situation and trends in the use of artificial intelligence in the defence sector

september 2025

With the collaboration of:

01 This abridged version has been extracted from the full report (written in Spanish). The full report and other complementary documents can be downloaded from the FEI website. This abridged version does not include bibliographic references, which can be found in the full report.

CONTEXT AND OBJECTIVES

The various technological approaches encompassed in **artificial intelligence (AI)** have undergone accelerated growth in the last decade that has increased their penetration in all layers of society. Today, it consciously or unconsciously affects billions of people and entities in all countries through the use of **AI-based applications to develop their daily activities**, a process that will intensify further in the future. The **global impact of AI as an enabling technology is enhanced by its integration with other technologies** such as microelectronics, robotics, neurotechnology, sensors, broadband communications systems, digital cloud services, cybersecurity, and other emerging technologies as quantum technologies or synthetic biology, with special emphasis on Implications for citizens through the widespread use of social networks.

Given this relevance, the **Forum of Innovative Companies** (*Foro de Empresas Innovadoras, **FEI**, http://foroempresasinnovadoras.com/*) developed a report in 2024 to assess the technological sovereignty of the European Union (EU) in AI and the way in which Spain could contribute to it in the coming years, recommending some actions for this purpose[02]. Following the work carried out in 2024 on the analysis of the strategic autonomy of the EU the FEI decided to focus the effort in 2025 by drafting a detailed **report on the impact of AI and its relevance for European technological sovereignty in the defence sector**. This document summarises the main ideas of the full report.

The analysis of **geopolitical determinants** that affect the global role of the EU influences its impact on the **use and deployment of AI in the defence sector** from several perspectives. It is based on the potential planning, tactical and operational revolution it entails in the conduct of military operations, with very relevant ethical and regulatory issues.

Geopolitical rivalries lead not only to a new **arms race**, but also to a global technological competition. Disruptive technologies such as AI, cloud computing, quantum technologies, and autonomous systems (for example, autonomous drones), are already shaping the new battlefield. In this scenario, **technological development will accelerate even more during the current decade**, and **AI**, as an **enabling and dual technology**, will play a preeminent role in all advanced weapons systems and decision-making systems in the military field.

Since the publication of the *EU Defence White Paper (Readiness 2030)* by the European Commission in March 2025, **the discussion in the EU Member States and in the EU institutions on the political, technological and budgetary priorities related to these issues has become increasingly prominent**. Therefore, informing society of the relevance that AI technology has for common defence and security, assessing its possibilities, limitations, and risks, as well as the need to be decisively involved in its development has become an

02 http://foroempresasinnovadoras.com/wp-content/uploads/2024/10/2024-10-15-Informe-FEI-sobre-autonomia-estrategica-en-IA-VCON-PORTADA.pdf

essential issue in the formulation of public European policies and for many Member States in the evolution of NATO commitments after the Summit hold in June 2025.

In addition, the debate on the structure and priorities of the new **Framework Programme for Research and Innovation (HE 2028-2034)** will begin in the second half of 2025 in the context of the future *Competitiveness Fund* to be approved before December 2027 within the negotiation of the EU multiannual financial perspectives 2028-2034 as presented in July 2025.

In this context, **greater effort is expected in the development of dual use technologies, including AI,** and proper funding and participation instruments should be redesigned to ensure their efficiency and adequacy in that context. Specifically, HE 2028-2034 will be closely interconnected with other EU programmes in the framework of the new **multiannual financial perspectives from 2028 onwards**.

Furthermore, it should be considered that, in the Spanish context, the Ministry of Defence will have to prepare in 2025-2026 the update of the *"Technology and Innovation Strategy for Defence (ETID)"* in which, for sure, **AI will play a very relevant enabling role** in all military systems.

The scientific and technological evolution of AI and the **introduction of AI-based products and services on the market** are occurring at a very rapid pace. For those reasons, the FEI set the **time horizon for its analysis in 2030**, it was open to considering forecasts or estimates up to 2035 relevant from the perspective of defence when there is a documentary basis for this as is the case with long-term defence projects.

The conceptual complexity of the use of artificial intelligence in defence requires a consideration of its analysis from several complementary dimensions. Specifically, the report adopts a multidisciplinary approach that integrates the technological, socioeconomic, strategic, tactical, and operational, and ethical and regulatory dimensions. Briefly, these dimensions address the following elements:

Technological dimension. It addresses the technological evolution of the AI in those areas with actual or potential relevance for defence within the time frame of 2030.

In this dimension, attention has been paid not only to AI's own techniques but also to its **convergence with other emerging technologies** such as microelectronics, robotics, communications and quantum sensors, neurotechnology, cybersecurity, edge computing, simulation (using, for example, digital twins), etc. The need to tune some of the AI techniques for their use in the defence context is also mentioned.

Socioeconomic dimension. The analysis carried out is based on the assessment of the volume of the AI market in defence based on the situation in 2024 and with estimates of

its foreseeable evolution until 2030 according to various reports from official entities and consulting firms; also, the changes related to its configuration and evolution in various countries are analysed.

The structure of the AI-related defence business sector is evolving very rapidly with frequent reconfigurations, mergers, and acquisition operations among its main players. This evolution is analysed in this document from **market reports** issued by various external entities, which do not necessarily coincide in their estimates, using the publicly available documentation on them.

In this dimension, a focused analysis has been carried out on the **way in which AI in defence is addressed in different R&D programmes in the national and international context**, with special emphasis on those of the EU and NATO and their consequences in the specific case of the participation of Spanish entities in them.

Strategic, tactical and operational dimension. This dimension addresses the way in which the conventional "battlefield" is involved in an accelerated process of digitalization, and it evolves from a digital battlefield (process in progress) to an "intelligent battlefield" (incipient process) with profound changes at the strategic, tactical and operational levels.

In this dimension, **special attention has been paid to the way in which AI is beginning to be used in open military conflicts**. Given that the military dimension of the use of AI is very broad and it is not possible to cover it in its entirety with unclassified data, this analysis has focused on three areas of undoubted current relevance. They are the following areas: the **space sector of defence**, the evolution towards **cognitive warfare** (in the broader context of hybrid warfare), and the growing **use of AI in decision-making systems** linked to autonomous or semi-autonomous weapons systems (LAWS) or components of broader *killer chains*.

Ethical and regulatory dimension. In this dimension, the emphasis has been placed on the ethical problems derived from decision-making processes in which human beings can be displaced by the growing use of AI algorithms in contexts of massive increase in the information to be handled, and the reduction of the time available to make sound decisions. Then, the interlinks with current AI regulatory approaches are described.

This dimension has acquired great relevance in recent years due to the **ethical consequences** related to the use of AI in the automatic identification of military targets or in its use in semi-autonomous weapons systems. It also discusses the **lack of a shared legislative and regulatory consensus** to address AI uses responsibly in military affairs.

Figure 1 schematically describes the **relationship between the dimensions** indicated above and some of the **key elements or factors** identified in each of them.

Figure 1. Dimensions used in the preparation of the report. Source: own elaboration.

These are **interrelated dimensions**; then, as the evolution of one of them affects the others, **impacts on defence should be analysed globally**.

Specific objectives of the report

With the expansion of AI applications, **humans are no longer the only agents involved in decision-making** in many areas of society. It is not even a matter of complex algorithms performing computations of complex models with greater efficiency and speed by taking advantage of high-performance systems, "intelligently" extracting data both from servers and from the Internet. Furthermore, these are systems that are capable of **"learning from their environment and evolving on their own"**; sometimes in directions unknown and surprising to the humans involved.

The emergence of **generative artificial intelligence** in society, first focused on the interaction, analysis and elaboration of text in natural language, and in the last years delving into the analysis and generation of content with a multimodal character (including audio, images, video, and computer programmes), has disrupted global markets.

Furthermore, the technological evolution of AI systems is enhanced by the gradual integration of **virtual reality** and **augmented reality** systems that are beginning to penetrate the mass consumption and professional markets. In the coming years, the evolution to integrate **holographic systems** and **neurotechnology** is expected to continue, although it is still in an experimental state. All of these are also inherently **dual technologies** that will be integrated into products and services traded in civilian and military markets.

The AI in defence will transform the nature of military conflict in which humans will co-exist and, to a certain extent, share decisions with previously trained machines and algorithms capable of learning from their own behaviour. We are heading "rapidly" from a "**digital battlefield**" to an "**intelligent battlefield**". The next ten years will witness this patched transition in which access to very powerful AI systems will be available to all the armies armies worldwide, although the development capabilities of the most advanced systems will be limited to some technological powers with the human and financial resources and political will to take advantage of that evolution.

In the context described above, the **specific objectives of this report** are as follows:

- To analyse the **technological bases of AI applied to the field of defence**, by emphasising its dual use and its relationship with other technologies.
- To assess **how AI is used today in military conflicts** (from open sources).
- To analyse the **use of AI-based systems related to defence in the EU** with analysis of interdependencies with supplier countries, and their evolution in the coming years.
- To determine **Spain's capabilities in AI for defence** and their foreseeable evolution in the EU context, taking a realistic stance.
- To draw up a set of **recommendations for action** for Public Administrations and companies as a basis for agreeing on measures in the respective areas of competence.

THE CONTEXT OF THE USE OF AI IN THE DEFENCE SECTOR

The use of artificial intelligence has spread rapidly to all economic sectors in the last decade, profoundly transforming society; but this is not an isolated phenomenon. **The relevance of AI cannot be separated from the digitalisation process** of which it is a part, which began years earlier. The **three phases or waves** (see figure 2) cannot be understood as completed processes that give way to the next phase, but **evolutions of the digitalisation process** that each one continues to follow its own specificities at higher performance, but at the same time with cross-impacts on their respective developments.

The **first phase** covers a period that spans until the beginning of the present century. Digitalisation was driven by the expansion of computing with cheaper and more powerful hardware and software systems that allowed the democratisation of access, fuelled by the progressive digitisation of information, the expansion of computer centres (initially centralised), and the automation of simple tasks (routine or well-defined), whether these are administrative or computational. **This phase cannot be considered finished** since, hand in hand with improvements in microelectronics (e.g. new types of chip packaging, lower consumption, higher speed, high frequencies) and distributed supercomputer architectures and networks, **processing capacities are continuously improved**.

The first phase made possible a **second phase** in which the techniques of capturing and analysing large volumes of data (*big data analytics*), supported by **high-speed networks**, as well as the sensing of the physical world with the deployment of **sensor networks** (*Internet of Things, IoT*), allowed the collection and deployment of database management and processing systems in the cloud. The expansion of **distributed and ubiquitous computing systems** and the consequent capacity to automate administrative or manufacturing processes of greater complexity is shaping today's society.

The **third phase** began gradually 20 years ago but has accelerated in the last decade and will continue to evolve very rapidly. This phase builds on the previous ones, facilitating **three decisive advances driven by the adoption of AI technology**. They are: the penetration of **generative AI** into society, allowing the generation of new information from (synthetic) data, text, voice, images, or videos; the expansion of **intelligent processing capacity** in all types of device ("*on the edge*" or "*in the fog*" computing); and the **intelligent automation of decisions** with the ability to support or replace human beings in many of them with the expansion of the so-called **intelligent agents**.

It is in this third phase that the attention of this report has been focused. However, it should be borne in mind that this third phase is based on the previous ones that do not disappear, deepening the process of digitalisation of society and, in particular, of the defence sector, whose adoption rates due to risk assessment for systems with lethal consequences are slower than those of the civilian sectors.

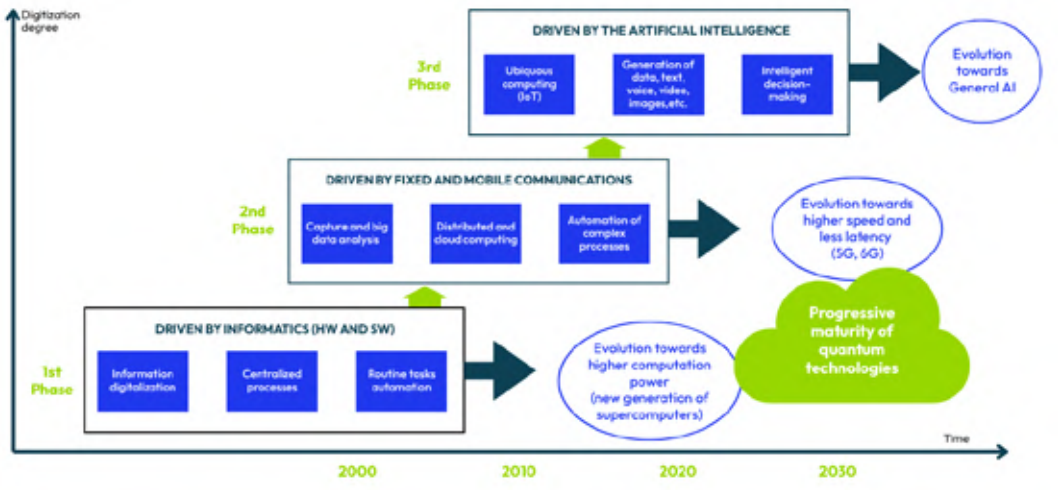


Figure 2. Main phases of the digitalisation process. Source: own elaboration.

Society is moving towards a **fourth phase of digitalisation** that is more distant in time but whose basic elements are already intuited. The evolution of computing capacity will continue in the next decade with the emergence of **quantum computing** (greatly accelerating processing capacity), with **6G mobile communications networks** (by offering much better performance in speed and latency), whose deployment will begin at the end of this decade, and with a **rapid evolution of AI's reasoning capacity.**

In the **defence sector**, the use of AI has reached a comparatively greater interest because behind its adoption is the ability to sustain **military supremacy** among the great powers, engaged in a race to achieve the desired competitive advantage through **AI deployment**. This interest is underpinned by the advantages that can be obtained by **introducing AI into multiple military systems** such as multidomain command and control, electronic warfare, intelligent management of the combat cloud, encrypted military communications, the data-driven design process of all military platforms, satellite constellations, or in lethal autonomous weapons systems, to name a few.

A transition to the so-called **"intelligent battlefield"** has begun to take place. Superiority in combat is achieved through the **synergy obtained from the massive generation and integration of real-time data** (based on a progressively *"transparent"* battlefield with millions of sensors in which the movement of troops and equipment is difficult to hide) **and the application of AI-based algorithms for decision-making.** This process is operationalised with the spread out of light command and control systems, and the deployment of multiple vehicles with autonomous or semiautonomous operation working in swarms.

As happens in all historical periods dominated by relevant military instabilities, technological development is accelerating; then, **the transition to the smart battlefield is unstoppable**, and its expansion will transform the nature of military conflict. This process will eventually expand across armies and overlap both conventional and digital battlefields, **profoundly changing planning, tactics, and military operations.**

Geopolitical relevance of AI

An additional factor to the purely technological one that gives AI a special relevance in relation to defence is its **geopolitical dimension**. Currently, the battle between great powers for mastering emerging technologies, of which AI has become a fundamental enabling technology, is based on a double set of geopolitical interests.

1. Accelerate the use of AI technology for the development of more advanced systems that achieve **improved competitiveness** and, with it, **supremacy in international** markets for

technological products and services, including the smart control of trade routes and the submarine data cables.

2. **Prevent opposing powers from having access to advanced AI technologies** that can be used to weaken their own position, whether in civilian or military superiority markets, by establishing export restrictions and sanctions on components, systems, or tools (e.g. for design or manufacturing) necessary for access to or development of AI-based systems; all of them driven by unilateral or multilateral decisions.

Both elements are combined in the **technological confrontation between the United States and China**, exacerbated in the field of semiconductor technology and AI, which is strongly dependent on the use of specific integrated circuits to get higher performance. **The geopolitical dimension of AI has acquired global relevance** with relevant impacts in third countries that became key players in the AI value chain, such as the EU, the United Kingdom, Taiwan, Japan, South Korea, India, Israel, Canada, Australia, Russia, and others; and, of course, it also impacts, as users of AI-based systems, in all countries in the world. For these reasons, the **adoption of AI in defence has been considered a priority for military powers**, with significant increases in the budgets allocated to development and acquisition of AI solutions.

The EU, anchored to the Western bloc and, from the defence perspective, highly dependent until now on NATO, **is constrained in a process of globalisation in which it has ceased to be a leader in many technological areas.** Therefore, the EU was well-aware since 2020 of the need of increasing its level of technological sovereignty as part of its long-term political strategy to achieve greater **strategic autonomy** in many areas, including defence and security.

European technological sovereignty in the defence sector

From the EU's perspective, **technological sovereignty has emerged as a key enabling element of strategic autonomy**, defined by the *European Parliament's Research Service* as the "*Ability to act autonomously, to rely on one's own resources in key strategic areas, and to cooperate with partners when necessary*".

Figure 3 schematically represents this **enabling role of technological sovereignty** based on the ability to secure the supply of critical products (such as rare earths), the capacity to manufacture components and systems (such as semiconductor devices), and access to knowledge. From a technological point of view, **digital technology is playing a growing role** in all of them.

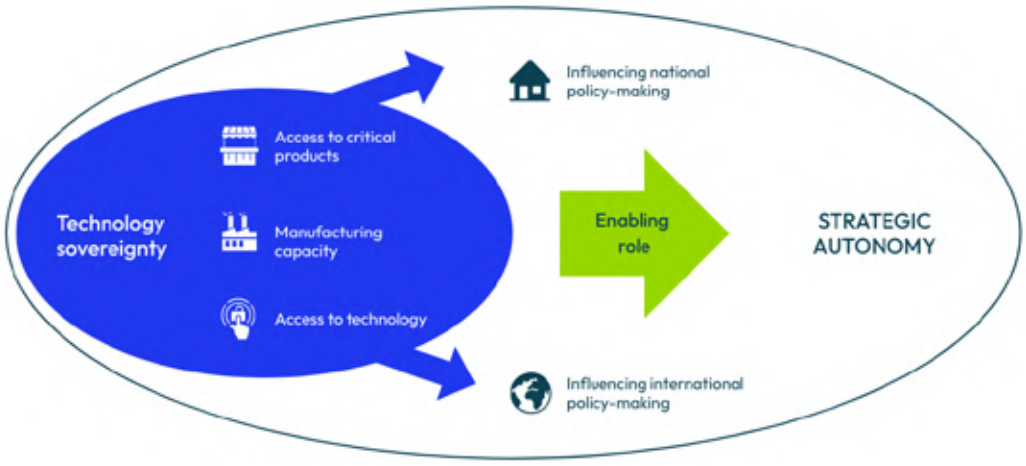


Figure 3. Relationship between strategic autonomy and technological sovereignty.
Source: León (2024)

The EU, depending on the position of technological strength it has at a given time in some key technologies, has developed specific **public policies** within the EU and in the international arena complemented by others in its Member States, **with the aim of enhancing its technological sovereignty** and reducing the existing gap with the leading countries.

However, **it is not possible for the EU to get full technological sovereignty in the AI domain**, especially if the EU's action is to be deepened in a framework of multilateral relations in which AI will be integrated into multiple manufactured products on which the Union's export capacity is based. Without **ensuring access to specific AI components** that Europe does not manufacture or with restrictions from suppliers for their integration and export to third countries, **the EU has limited technological sovereignty in AI**.

This weak EU starting position is also reflected in **military markets** where European technological dependence, as the case of AI semiconductors and the provision of AI services based on digital platforms for decision-making (i.e. on command and control) reveals, poses an urgent challenge to be addressed with additional resources and sustained political will. Notice that in this field, providers also impose some constraints on the future use of acquired military systems as the Ukraine war has clearly shown.

The civilian and defence realms are intertwined in multiple technological applications in which dual characteristics emerge as key factors**.** In fact, this situation occurs in the case of AI with the use of large language models (LLM), AI chips, multimedia content generation, or tools for synthetic data generation that, although initially developed for civilian markets, are increasingly used in the defence sector embedded in advanced military products.

This adoption could imply some adaptations or tuning processes to comply with military contexts and related risks.

A direct consequence of this fact is the influence it has had on governments in defining **access strategies** imposed on other countries for the use and control of technologies such as AI in civilian markets. The cases of China and the United States show the trend to strengthen the control of technology transfer between the civilian and military spheres, even when different approaches were applied.

In the *United States*, the objective of **civil-military integration** is to increase cooperation between the US government and tech companies in research and development (R&D), manufacturing, and maintenance operations. The chosen approach was based on large tenders in defence contracts for providing innovative weapons systems or platforms, or smaller disruptive research projects funded from agencies such as ***DARPA*** (*Advanced Defence Research Projects Agency*), in which participation is also sought of universities and research centres as part of a complex defence ecosystem. In addition, a **network of national laboratories** financed directly by the US federal budget developed advanced defence projects in emerging technologies with a high degree of confidentiality.

China, **as a government-orientated and directed plan,** transitioned in recent years from the concept of **"civil-military integration" to "civil-military fusion"** with the creation of the Central Commission for the Development of *Civil-Military Fusion* (MCF) in January 2017. China is actively integrating AI into its military strategy as a critical enabler of future *"smart" warfare*. It is not easy to assess to what extent the information control system used by the Chinese government will influence the ability to train its AI systems. If anything, the various restrictions on the export of dual-use high-tech imports to China (such as semiconductors or some software tools) may slow, but not stop, the development of military AI.

As **competition between the United States and China intensifies**, there is a growing risk that **AI-enabled weapons** will proliferate without a common regulatory approach or consensus on their use by involving many other countries.

Several geopolitical **events have emerged** in 2025 which potentially affect the use of AI in defence in the European context:

- Trigger of a **tariff war** provoked by the United States and answered by other countries, including the EU, on a multitude of products, both raw materials and technological products, with continuous changes in the proposed or applied percentages, generating uncertainties and perturbing world trade.

- The United States' position strongly opposes European digital regulation and, expressly, to the **AI regulation that imposes conditions on USA companies** in their operation in

the EU. Position which is, partially shared by European firms, which could slow down the implementation process of the AI regulation.

- A unilateral change in the **attitude of the United States to support Ukraine** without the EU, which, from a technological perspective, has led to threats to prevent the use of essential technologies to feed the intelligence of the Ukrainian army or the deployment of essential weapons to protect against air attacks.

- The aim of seeking a **solution to the conflict in Gaza** is to not count on the EU but to provide Israel with sophisticated weapons or accelerate the development of others with possible increases in the already existing distance from the EU. The consequences of the conflict have also provoked in some EU member States the reduction of military cooperation with Israel.

- Agreement in the NATO Summit to **increase defence expenses** to the 5% of the GDP of the member countries of NATO up to 2035 (3,5% focused on military capacities and 1,5% on infrastructures, cybersecurity and other expenses indirectly related to defence) with an intermediate assessment in 2029.

The **EU response** has been based on extensive discussion among Member States to conciliate political and economic wishes and derived in the adoption of various measures at much higher speed than it was usual in the past.

1. **Strategic compass for competitiveness**. In January 2025, the European Commission presented a framework document for improving competitiveness with a new roadmap to restore Europe's dynamism and boost economic growth.

2. **"Omnibus" package of simplification**. In February 2025, the European Commission presented a package of measures that seeks to reduce the administrative burden on EU companies, ensuring that they can remain competitive without compromising their sustainability obligations.

3. **Rethinking the Community budget**. In February 2025, the European Commission presented the communication entitled "*The road to the next Multiannual Financial Framework MFF*" with the aim of kicking off the debate to transform the future EU budget.

4. **Measures towards the rearmament of the EU**. On 4 March 2025, the President of the European Commission announced the "*European Rearmament Plan*" focused on using all available financial levers to drive Member States to rapidly and significantly increase spending on defence capabilities.

5. On 19 March 2025, the Commission presented the "**White Paper" on the future of European defence / Readiness 2030** which triggered an in-depth discussion process on European defence priorities and funding. It includes the identified priorities in European defence technology systems on which additional investments should be concentrated. Priorities were identified in air and missile defence, artillery systems, including precision strike capabilities in depth, missiles and ammunition drones and anti-drone systems, strategic support elements, including in relation to space and the protection of critical infrastructure, military mobility, the cyber space, and AI and electronic warfare.

6. A relevant step forward was the approval by the EU Council in May 2025 of the **Regulation on *Security Action for Europe (SAFE)*** to raise up to EUR 150 billon in the capital markets. The intended objective of SAFE is not only to provide access to financial resources but also to strengthen and integrate the European defence market**. The SAFE Regulation** includes the condition that *"joint procurement contracts should contain the requirement that the cost of components originating outside the Union, the EEA EFTA states, and Ukraine should not exceed 35 % of the estimated cost of the components of the final product*".

7. On 17 June 2025 the European Commission has adopted the **Defence Readiness Omnibus**, a comprehensive package aimed at establishing a defence-readiness mindset across the European Union. This initiative lays the groundwork for facilitating up to EUR 800 billion in defence investments over the next four years, enabling Member States and industry to respond swiftly and effectively to growing threats.

8. On 10 July 2025, the **draft regulations of the Competitiveness Fund and Horizon Europe** for the period 2028-2034 were accessed, consolidating the interest in giving greater weight to the development of dual-use technologies.

9. Finally, on 16th July the European Commission has published its **proposal for the MFF 2028-2024** which will frame the negotiation process for the next two years.

All these measures produced in a few months drive the EU political will to create the **defence scenario** which is needed to address the present and future **common security challenges**, where technology, and specifically AI, will play a prominent role.

AI EVOLUTION AS A DUAL USE TECHNOLOGY

From data to knowledge

The European Commission defined **AI systems** as *"software systems (and sometimes hardware) designed by humans that, faced with a complex objective, act in the physical or digital world perceiving their environment through the acquisition and interpretation of structured data,*

semi-structured or unstructured, reasoning with knowledge, processing the information derived from this data and deciding on the best actions to take to achieve the objective". Depending on the complexity of the task that artificial intelligence solves, the literature distinguishes **three types of artificial intelligences**: **specialized AI, artificial general intelligence** and **"singularity"**.

Today, there are many **specialized artificial intelligences** - also known as narrow or weak AI- that are highly effective at performing specific tasks. These systems can evolve and improve by interacting with other specialised AI. Through processes of interaction, aggregation and negotiation, they gradually advance towards the resolution of more complex tasks. The **artificial general intelligence (AGI),** what is known also as strong AI, is capable of replicating a full range of human cognitive abilities, such as the resolution of complicated and heterogeneous tasks, planning, learning, reasoning or the ability to abstract and generalise.

In recent years, the concept of **generative artificial intelligence (GAI)** has emerged. It refers to a technology that can generate texts, images, videos, computer programmes, among others. It enables the development of AI systems (or multi-agent systems) that can collaborate to perform simple or complex tasks. At the most advanced level is the **technological singularity**, which is the ability of an artificial intelligence system to generate another artificial intelligence better than the one that already exists.

In this revolution, **AI is and will be accompanied by other enabling technologies**, such as the Web and Web 2.0, the Internet of Things, massive data storage, and cloud computing; blockchains; robotics, and the metaverse, which will take us to a hybrid reality, between the physical and virtual.

At the same time, the **integration of AI with other emerging technologies** such as quantum computing, neuromorphic computing, neurotechnology, or chips implanted in humans to increase their physical, cognitive, and communication capabilities with other devices are also contributing to this technological revolution.

In this setting, **real-time decision-making** requires a shared interpretation of both the data and metadata being exchanged. Heterogeneity problems appear in communication protocols, data syntax, and model semantics and they cause interoperability issues when exchanging and sharing data and making decisions. In addition, other important aspects must be considered, including data governance, data duplication, data inconsistencies, lack of bias, levels of certainty, data granularity, and the language used to represent the data. **Non-technical dimensions** come into play, including regulatory aspects related to compliance, intellectual property and access rights, and contractual frameworks between suppliers and customers.

One widely used framework for conceptualization the progression from raw data to deeper understanding is the **pyramid of knowledge**. The **pyramid of knowledge** helps to understand how information is acquired, organized, represented, and processed

hierarchically, from the most basic to the most complex levels. It has four levels: **data**, **information**, **knowledge**, and **wisdom** (see Figure 4). **Each level of the pyramid** is built upon the previous ones, progressing from raw data to decision-making at the top level. The example in Figure 4 on $C0_2$ (right) shows how raw data is progressively transformed into useful knowledge for decision making.

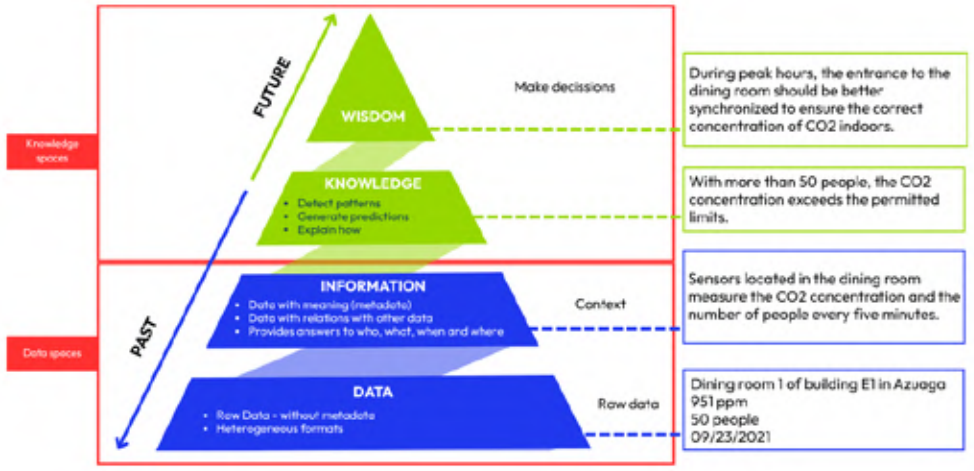


Figure 4. The knowledge pyramid: from data to decision making. Source: Own elaboration.

To learn, reason, or make correct decisions in accordance with the regulatory framework that is appropriate in each case, it is necessary to analyse the **iterative processes that make up the data value chain that allows data to be used for decision-making** (see Figure 5). This approach is pushing a data-driven engineering process where **digital twins** of products promise shorter and more flexible development life-cycles.

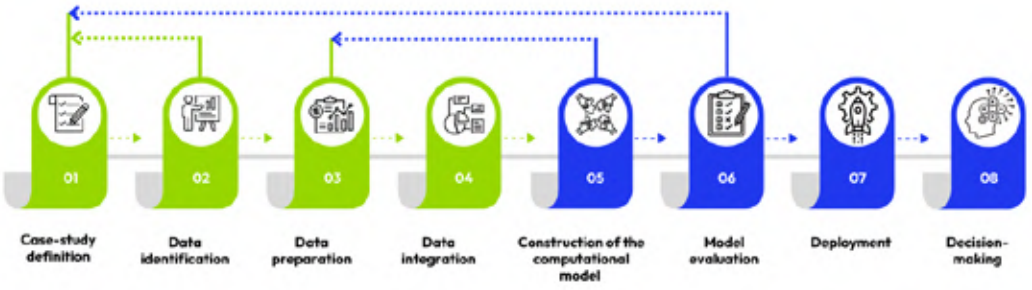


Figure 5. Data-driven value chain. Source: Own elaboration.

The role of models

It is important to remember that the evolution of AI is closely tied to advancements in hardware and the growth of data volumes, and the development of computational models and algorithms. **Computational models are abstractions of the physical or virtual world,** and contain the domain knowledge essential for the AI systems to learn, reason, make decisions, adapt their behaviour and provide traceable explanations for those decisions. These models are built using different techniques, giving rise to the the main **areas of AI**: **symbolic AI**, **sub-symbolic AI**, and **generative AI** as shown in Figure 6.

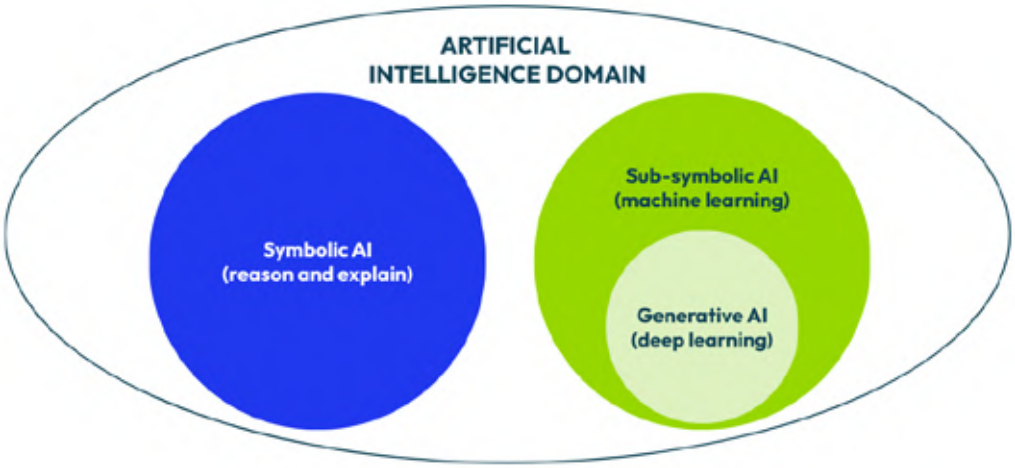


Figure 6. Main areas of artificial intelligence. Source: Gómez-Pérez (2024) https://raing.es/pdf/publicaciones/discursos_de_ingreso/Discurso_Ingenieria_Ontologica.pdf

Symbolic models belong to the area of AI focused on knowledge representation and reasoning. They are grounded on *Boolean algebra* (1854) and the principles of logic, which enable these systems to perform reasoning and provide explanations of their inferences and deductions. During the 20th century, these techniques played a key role in the development of *expert systems*. Faced with limited data and computing resources, engineers acquired knowledge from domain experts and specialized documents. The most commonly used techniques are: logic, rules or heuristics, taxonomies, ontologies, and knowledge graphs. These approaches rely on symbols to define the key concepts and relationships between them within a domain. Then, algorithms infer new data and knowledge from existing information, specifically through deductive inference to narrow down search options. In this way, they effectively reduce the combinatorial explosion in the search space.

AI techniques that learn and predict new knowledge from large datasets are in the area of **sub-symbolic AI.** This field has two main branches: one based on statistic,

which generate patterns using probabilistic models commonly referred to as **"classical machine learning"**, and another inspired by the brain's structure and function (known as **"deep learning"**).

Machine learning techniques are generally classified based on the problem type being addressed and the availability of labeled data. **Supervised learning** involves training with labeled data, while **unsupervised learning** works without labeled data. Additionally, in situations where models need to be frequently updated during operation based on their current state and potential actions, **reinforcement learning techniques** are used**.**

Generative AI is based on Deep learning. Deep learning is a branch of machine learning that uses artificial neural networks with many layers (called deep neural networks) to automatically learn patterns with billions of parameters from large datasets. Deep learning plays a crucial role in modern AI models. Unlike traditional machine learning, which often requires manual feature extraction, the new architectures and algorithms have been "fed" with massive volumes of data, allowing them to automatically discover complex patterns, features and relationship. This capability has significantly improved their performance in tasks such as understanding and generating human language, images, videos, music, computer programmes, among others.

A major breakthrough in this evolution was the introduction of the **Transformer architecture**, which introduced two key concepts: **tokens and attention**. Tokens represent the minimum unit of meaning while the attention mechanism relates all words in a sequence. Together, these innovations revolutionized natural language processing by enabling the creation of powerful language models by capturing patterns and contextual relationships within texts. The size of the language models is measured by the number of **parameters**. Language models, in more advanced versions, have given rise to Large Language Models (LLMs), Diffusion Models, Foundational Models, Small Language Models, Quantised Models and Distilled Models. Most of the foundational models are open and can be downloaded from *Hugging Face*.

Prompt engineering is the technique used to guide a language model toward generating the desired answer. To produce reliable, trustworthy and accurate responses, prompts must be carefully crafted and designed. However, models produce **hallucinations** that lower the credibility of the responses. Hallucinations are invented responses, factual error, incoherent responses, among others. To address this issue, *Retrieval-Augmented Generation* techniques enhance the model performance with additional context beyond its original training data. By retrieving relevant information from external sources, the model can improve the accuracy and credibility of its outputs.

In addition to hallucinations, another critical challenge in language model is **bias**. Bias refers to the presence of unfair, unbalanced or prejudiced patterns in a model's response

that is caused by the presence of stereotypes or inequalities in the training data related to gender, race, culture or politics, among others. Addressing bias requires data curation and continuous evaluation to detect it at an early stage, helping to prevent harmful outcomes and decisions that could have negative impact on individuals or groups. It is well known that some gender and racial biases are necessary, to some extent, for some medical diagnoses and for the analysis of human genetics. But bias is inherent to human beings and influences decision-making.

In recent years, the **neuro symbolic approach has appeared, combining symbolic AI with generative AI by injecting knowledge from ontologies and knowledge graphs into pre-trained LLMs.** The structured factual data knowledge graphs can be leveraged to train and validate the veracity of the generated texts, to reduce hallucinations, and to provide transparency by tracing the source of the answers. Fine-tuning LLMs with knowledge graphs helps reduce bias and improves accuracy in specific domains.

In any case, this implies that **building models is not only expensive but also risky**. In the case of its use in defence, some questions are crucial to adopt them: Would it be possible for an army to buy a decision model trained in another country, friendly or neutral, without being able to be sure of the conditions and dataset with which it has been trained? Is it possible to ensure that the model does not have backdoors?

The need to answer those questions has motivated the launching of **several projects to adapt LLMs, prompt techniques and generative AI tools** to cope with defence requirements.

Hardware/Chips AI for defence

The basic concept for measuring the degree of advancement of microelectronics is the **technological node**, which refers to the **minimum size of the features of a chip manufactured by a specific process**, expressed in nanometres. This parameter defines key aspects such as operating frequency, density per 2-millimetre, wafer yield, and energy consumption. This is not an exact physical measurement, but it is used to distinguish between different generations of chips.

The **reduction in the size of devices** allows many more devices (more complex circuits, true systems) to be integrated in the same area, so as the size of the node decreases, the cost of designing the chip increases, not linearly. However, the manufacturing costs of prototypes are higher because the amortisation of equipment and the cost of masks (more complex processes and smaller dimensions) are higher. Figure 7 (right) shows the **increased cost of chip design** (design engineering plus manufacturing, encapsulation and prototype testing).

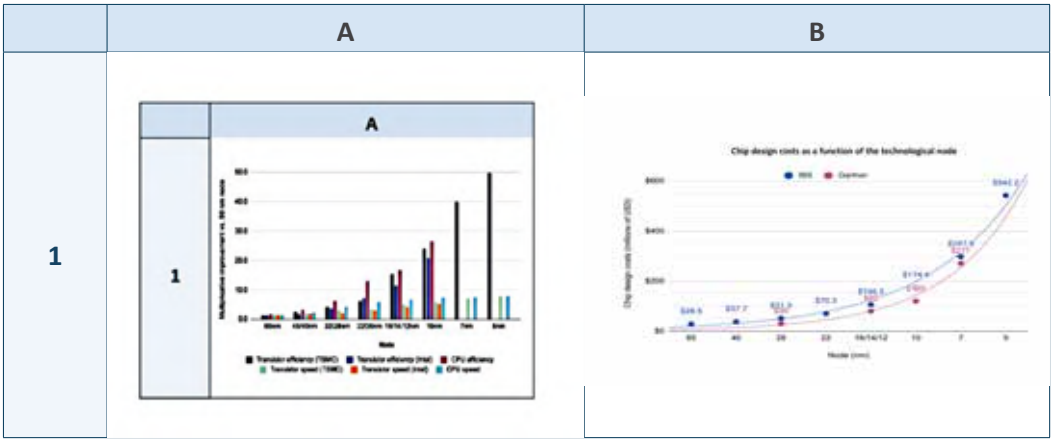


Figura 7 (left.) Efficiency and speed compared to 90nm node; (right) Cost of designing a chip based on the technology node. Source: Khan & Mann (2020) https://cset.georgetown.edu/wp-content/uploads/AI-Chips%E2%80%94What-They-Are-and-Why-They-Matter-1.pdf

The *IEEE Rebooting Computing Initiative's International Roadmap for Devices and Systems (IRDS*) defines key trends in semiconductor technology (see Figure 8). It does so through three complementary approaches: **More Moore** drives conventional scaling, **More than Moore** integrates new functionalities, and **Beyond CMOS** investigates future replacements for traditional computing technologies. Notice the relevance of *System-on-Chip (SoC*) in several technology nodes, and the systems integrated in a single package, *System-in-Package (SiP*) for different types of chips.

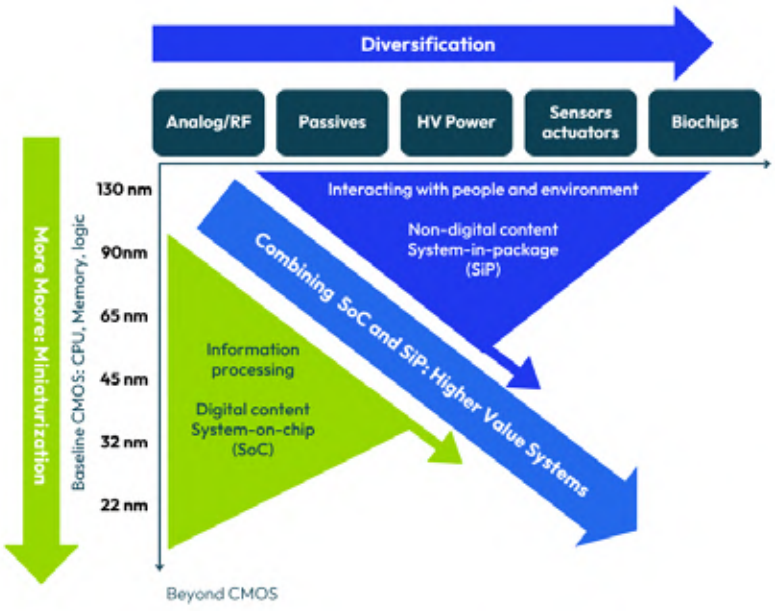


Figure 8. Roadmap for integrated systems Source: IRDS (2023). https://irds.ieee.org/images/files/pdf/2023/2023IRDS_BC.pdf

Chips for Defence Applications

The requirements that chips must meet for use in defence are **more demanding than those for civilian use**. Among its characteristics are:

- **Temperature range and environmental tolerance:** the operating temperature can vary between -55 ºC and +125 ºC (sometimes up to + 200 ºC), while those for civil use usually operate between 0 and 70 **ºC. They must be resistant to shocks and vibrations** under extreme conditions. They must be protected against moisture and corrosion from salt spray.
- **Reliability and Longevity:** Very low failure rate in mission critical systems. The useful life should be 15 to 30 years.
- **Security and Anti-Tampering**: they must have secure boot systems, self-destruct mechanisms, and hardware encryption. They must have electromagnetic protection (EMI/EMC). Your supply chain must be secure with strict tracking, often integrated into secure factories.
- **Radiation Hardening (rad-hard)**: designed to withstand gamma rays, cosmic rays, and neutron bombardment. Total ionizing dose tolerance between 100 Krad and 1Mrad.
- **Manufacturing process and materials**: The technological nodes are larger than those of commercial chips for robustness (90 nm, 120 nm, 180 nm). Very small nodes (5nm) are very sensitive to radiation, so they do not meet the above requirements. The substrate material can be SOI, silicon carbide (SiC), gallium nitride (GaN), which withstand radiation and high temperatures better than conventional silicon. The package must be ceramic, sealed with metal to encapsulate the chips and protect them from electromagnetic interference (EMI) and hardware attacks.
- **Cost and availability**: They cost 10 to 100 times more than equivalent commercial chips. They have a low volume of production, organized by custom orders to classified factories. Finally, their availability is restricted, controlled by governments.

Semiconductors play a crucial role in various military applications. Their small size, low power consumption, and high reliability make them ideal for military technologies that require compactness, efficiency, and durability. **Examples of dual use** are the chips used in 5G antennas or car radars; high-performance processors as these are used in data centres for AI training and in military simulations or advanced cryptography; an AI chip used in a smartphone may be the same one used in image Reconnaissance systems in military drones.

GaN has been used for some years in defence chips for its properties of high electron mobility and saturation speed, which enable the development of high-frequency devices**.** They operate at high voltages without compromising performance in high-power applications. They also dissipate heat effectively and can offer high-power outputs in small physical spaces. The **main applications** are: 1) Missile guidance systems; 2) Radar Systems; 3) Images and surveillance; 4) Secure military communications (millimetre wave links provide a large secure

bandwidth (e.g., communication in the 75-110GHz W-band); 5) Directed energy weapons (high-power millimetre waves can be used as weapons to disable enemy electronic devices).

Types of chips for use in AI

AI chips are defined as h**igh-efficiency and high-speed data processors suitable for training or inferencing AI models**. They can handle operations with multidimensional arrays (called tensors) on a large scale by using parallel computing since AI models (neural networks, deep learning, and transformers). Depending on their construction, AI chips can be classified into **Graphic Processing Units (GPUs**); **Field Programmable Gate Arrays (FPGAs)**; and **Application Specific Integrated Circuits (ASICs),** which include AI accelerators, neuromorphic circuits, and Artificial Intelligence Memory in Computing (AIMC). Figure 9 shows these relationships between the different types of AI chips.

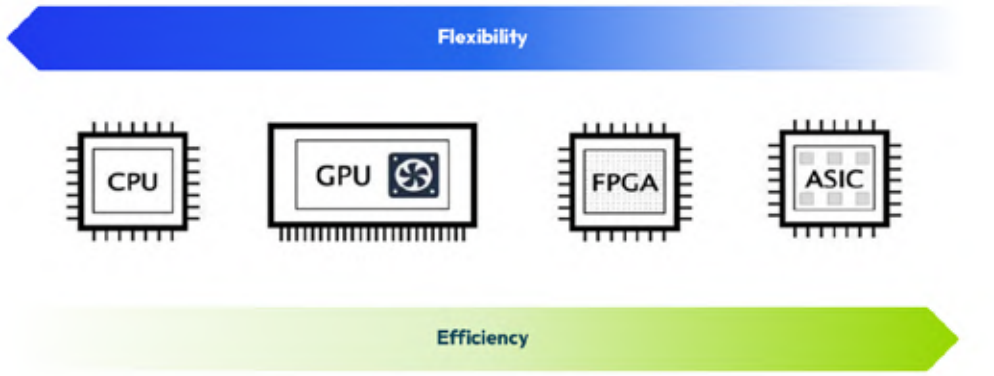


Figure 9. General classification of AI chips according to their construction. From left to right, they increase their energy efficiency; From right to left increase your flexibility.

The **GPU is an image processor** that displays the information to be displayed, provides scan signals to the screen, and controls it. The original intent of GPU design was to address the need for large-scale parallel computing in image processing. It is used in the training phase of AI models. Moreover, its hardware structure cannot be flexibly configured, as it is fixed; and running an algorithm is less efficient on a GPU than on an FPGA, for example.

GPUs are the predominant type of AI chip in cloud AI data centres, although combinations of CPUs with AI Accelerators (chips with specialised ASIC architectures) are increasingly being used. The most widespread GPUs today are those from **Nvidia**. Most cloud data centres are home to the H100 and H200. In 2025, the B200 will begin to be installed, substantially improving the performance of the H100. *CUDA software platform* helps developers utilise the many cores of a Nvidia GPU.

An **ASIC is a chip that is optimised and customised for a specific application**. ASICs for specific AI tasks achieve better performance and energy efficiency compared to GPUs and CPUs.

Both ASICs and FPGAs involve long and expensive design cycles, but ASICs have optimised hardware, at the cost of losing flexibility to implement changes. They are specialised in the **deployment and run of trained machine learning models**, enabling real-time predictions and decision making across multiple applications. That is, they efficiently process the input data through AI models to generate fast and reliable predictions: They are suitable for inferences. **Dedicated chips (ASICs) are more efficient than GPUs**, leaving GPUs for training with large amounts of data. It is estimated that by 2030 the most widespread solution will be a specialised chip architecture (ASIC) and FPGA with optimal performance for specific AI tasks.

In addition to the military requirements for equipment at the edge, there is a need to be able to **perform inferences** (in some, very few cases, also training) **locally**, with minimal latencies and little access to the network (intermittent or disconnected). For inference at the edge to be possible, the models must have been optimised for resource-constrained devices. The biggest challenge facing **AI chips at the edge** is **power consumption**. These chips are usually powered by very small batteries (*button batteries*) and must also have a significant duration, as it is not easy to replace them because, usually, they are located in environments with difficult access.

Public funding projects for AI chips for Defence

DARPA (*Defense Advanced Research Projects Agency*) manages several AI chip programs for defense:

- **CHIPS Programme** (*Common Heterogeneous Integration and IP Reuse Strategies*) seeks to create an ecosystem of modular and reusable IP blocks (intellectual property, IP), which can be integrated into systems using existing and emerging integration technologies, facilitating more flexible integrated circuit designs and reducing development costs and times.
- **IDEA Programme** (*Intelligent Electronic Assets*) seeks to develop a general-purpose hardware compiler that allows automatic translation, without human intervention, of source code or schematics into physical designs of integrated circuits in less than 24 hours. This aims to accelerate the development of next-generation electronic systems and reduce the reliance on large, specialised design teams.
- **DARPA.MIL SAHARA Programme** (*Structured Array Hardware for Automatically Realized Applications*) aims to expand access to U.S. manufacturing capabilities to address challenges in the secure development of custom chips for defence systems. The program seeks to automate the conversion of FPGA designs to structured ASICs, improving performance and reducing power consumption in military applications.

The European Commission and European Agencies, through the **European Defence Fund (EDF**), and the **European Defence Agency (EDA)**, have launched calls for research and development projects in microelectronics and semiconductors, seeking to strengthen European technological autonomy in key sectors such as defence and space. Sources consulted do not detail specific projects. In addition, in Europe, the **European Space Agency** (**ESA**) funds

projects aimed at developing semiconductor components capable of operating in extreme space environments, including resistance to radiation and extreme temperatures.

SOCIO-ECONOMIC DIMENSION OF AI IN DEFENCE

Military AI market

The use of artificial intelligence in the defence sector not only transforms security and military strategy but also **drives economic and industrial development**. The integration of AI in defence systems generates an innovation ecosystem where the technological, aerospace, and cybersecurity industries converge, strengthening technological sovereignty and reducing dependence on external suppliers. Furthermore, i**nvestment in AI for defence stimulates the creation of highly skilled jobs** in key sectors such as software engineering, robotics, and data analytics. In addition, it improves the competitiveness of companies in the global market, promoting the export of advanced solutions in security and dual-use civilian-military technology.

The **socioeconomic impact** of the AI depends on three key components: **software**, **hardware**, and **services**. Software development (50% of the market) stimulates the creation of specialised employment in areas such as data analysis and advanced programming, while hardware manufacturing boosts technological industries and increases the demand for high-tech components, benefiting local and international economies. On the other hand, associated services generate new economic opportunities in strategic consulting, training, and technical maintenance, thus strengthening the labour market and promoting greater investment in technological innovation.

The AI market in the military is experiencing remarkable growth. According to *The Business Research Company*, it has grown at a solid CAGR of 16.72% since 2019, reaching USD 9.671 billion in 2024 and projects that it will reach a value of USD 19.74 billion in 2029, with a CAGR of 15.1%. *Precedence Research* (2024) estimates that the global AI market in the military was USD 9.56 billion in 2024, and that it will grow to USD 10.79 billion in 2025, pointing out that it will reach USD 32.17 billion by 2034, with a CAGR growth rate of 12.9% between 2024 and 2034. This growth is driven by the increased adoption of **unmanned aerial vehicles (UAVs), military modernization programs,** and an **increase in defence budgets** globally.

Markets by region

Military AI market shares by region in 2023 reveal that **North America represented 36%, Europe 30%, Asia-Pacific 24%, Latin America 6%, and the Middle East and Africa 4%.** Europe, with 30% in 2023, has a prominent weight, although the development and operation

of its systems may depend on components, software, and Intellectual Property (IP) from other countries, mainly the US in the field of NATO. Europe's share is also growing steadily, suggesting that the defence budget incorporates more AI-powered capabilities.

In 2024, the combined market of the **top three European nations, the** *United Kingdom, France* and *Germany*, for AI in defence generated revenues of USD 2,348.8 million according to *Grand View Research*. By segment, **software was the offering with the highest revenues in 2024**, consolidating itself as the strongest area of the market. However, **hardware is the most lucrative segment**, registering the fastest growth during the forecast period. The military AI market in Europe is expected to reach a projected revenue of USD 4.09 billion by 2030. It is important to consider that if EU countries continue to purchase large quantities of systems and technologies – be it hardware, software or services – from non-EU suppliers, the European defence industry will continue to be smaller than desirable.

A relevant indicator is the publication of **AI-related patents in the aerospace and defence industry.** Since 2020 (data from *Global Data Patent Analytics*), the *United States* accounted for 44%, followed by *China* (37%) and *South Korea* (7%). The aggregate of the *EU*, the *United Kingdom* and *Turkey* **only represents 5.4% of patents filed in this area**.

There is no unified public figure that accurately reflects the volume of AI market in the military sector in Spain. **In 2024, Spain's defence investment budget was EUR 13.1 billion**. There is no doubt that **AI already plays an important role in the Spanish defence industry** and in the domestic market. Applying a conservative factor of 0.3%, it is estimated that AI could have represented potential revenues of more than EUR 40 million in Spain. According to NATO data from 2021, Spain was present in large programmes in which AI plays a relevant role, such as Aegis (AMD), Barracuda (UAV), BlueScan (ASW), Future Combat Air System (FCAS, aerial platform), Harpoon Block II (missile), Patriot (AMD), RQ-11 RAVEN (UAV), SWORD (simulation), ScanEagle (aerial platform) or nEUROn (aerial platform).

The 2025 report by the *National Office for Foresight and Strategy* under the *Presidency of the Government of Spain* highlights the **Air Force's MPC16 project** for the predictive maintenance of Eurofighter aircraft, the **Army's Predictive Logistics System (SILPE**), the digital twin integrated into the F-110 Frigates or the **On-Board Predictive Maintenance Module (MAPRE)** for Navy ships. Furthermore, the Spanish Ministry of Defence has created ***Idoia***, an AI assistant developed by the C*entre for Information and Communications Systems and Technologies (CESTIC)* and ***Imbox***, a specific instant messaging application for the Ministry of Defence that already had nearly 12,000 users in 2024. Furthermore, the Ministry of Defence has begun a strategic process to **integrate AI systems into Army decision making**, both at a technical and operational level. In 2024, technical needs were defined to investigate how to automate this process using AI. Currently, the initiative is in an initial phase.

Characterization of the AI for Defence Industrial Sector

Most of Europe's defence industry is located in its western member states, especially the UK, France, Germany, and Italy. Normally, these countries support the EU's defence industrial initiatives if they think their own industries will benefit. There is no EU defence company in the top 10 in the world by revenue in 2022. Among the top 20 can be counted three Europeans, *Leonardo*, *Airbus*, and *Thales*.

The **Spanish defence industrial and technological base (BITD)** had more than 520 companies in 2021, although only about 350 provided products or services in the field of defence. The number of direct jobs in defence was around 22,000 direct jobs, and the associated turnover was EUR 6,300 million, which accounted for 15% of its total sales (civilian and military). This activity has a driving effect mainly in large programmes for weapons platform development, especially for Tier 1 and Tier 2 companies, but also for other subcontractors and SMEs in the supply chain. The latter categories represent about 85% of the total number of companies in the Spanish defence industry. **In terms of market share, 1.5% of the companies represent 75% of the entire market.**

The **annual report** of the *Directorate General of Armament and Material* of the Spanish Ministry of Defence (2024) points out that in 2022 the total sales of the national defence industry were EUR 7,435 million, with indirect sales to the Spanish Ministry of Defence of EUR 2,023 million. If the national part of *Airbus*, *Rheinmetall (EXPAL)* and *MBDA* is considered, the sales figures of the Spanish defence industry almost double. Although there is no unified official figure, AI in defence is estimated to have generated more than EUR 40 million in 2024, based on 0.3% of the national defence budget. Investment is growing, driven by digital transformation and the demand for advanced capabilities.

Several Spanish companies in the defence sector are incorporating AI solutions into their projects and systems. In 2024, *Indra, GMV, Airbus Defence and Space Spain, SENER, Expal, Tecnobit (Oesia Group), Amper, Swarming Technologies & Solutions (Zelenza Group), Escribano Mechanical & Engineering,* and *Aertec* should be highlighted. Important multinational companies, through their subsidiaries and offices in Spain, contribute to technology transfer, innovation, and competitiveness in the defence sector, strengthening both local capacities and international collaboration in strategic projects. The most relevant are mentioned:

- **BAE Systems** has established a subsidiary in Spain.
- **Thales** has a strong presence across several companies,
- **Leonardo** actively participates in aerospace and defence programmes.
- **Lockheed Martin** has offices and support units in Spain to manage projects and contracts with the Armed Forces and government agencies.
- **Boeing** has a development centre (*Boeing Research & Technology Europe, BRTE),*

- **Raytheon Technologies** is represented in Spain through subsidiaries or local units that allow the integration and support of defence systems, such as missiles and radars.
- **Northrop** operates with regional offices that facilitate project coordination, contract support, and participation in collaborative initiatives with local entities.

Public support for R+D is one of the strategic tools for developing a technological and industrial base in the defence. Each country has a very different approach when comparing the % of public funding for R+D dedicated to defence, as illustrated in Figure 10.

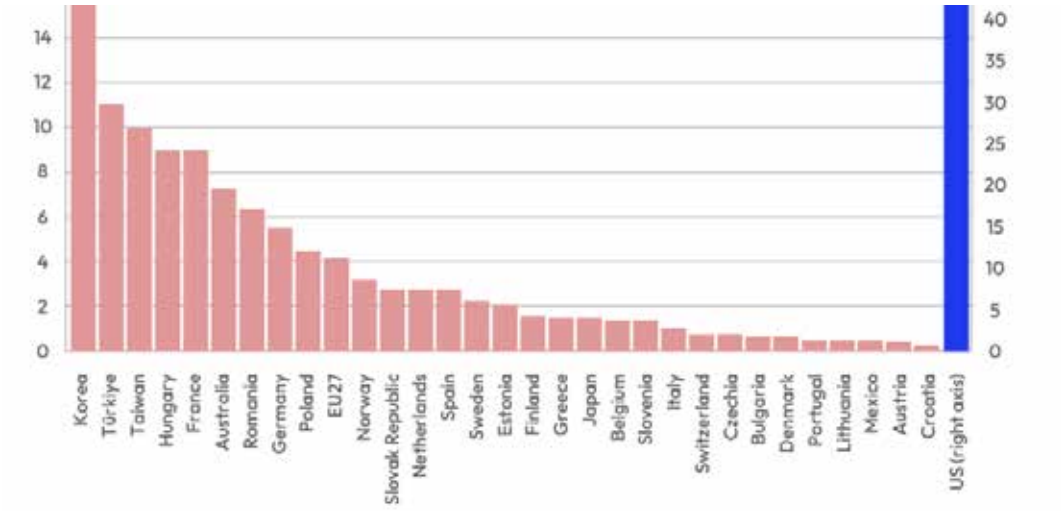


Figure 10. Public funding for R&D by nation. Source: Bruegel (2024)

This vision covers public support for AI. In the US, 95% of federal government funding for AI is under the heading NAICS 54 (designation for professional, scientific, and technical services). 84% of the total value of funding under NAICS 54 is tied to contracts related to the Department of Defence (DoD). The federal government's total investment in AI in 2022 was approximately USD 3.3 billion, complementing in a fully directional way the massive investments already made by the private sector in that country. This pattern is similar to that in China, where investments combine the objective of satisfying strategic security needs while boosting the competitiveness of the industrial sector. China has, specifically, an ***AI Strategy for Defence and Security.***

The EU segments investments between **community and national institutions** (including regional) and the lesser alignment with security objectives. Therefore, the EUR 1,000 million per year declared in 2018 could be added to comparable amounts in some individual countries.

Venture capital (VC) has played a pivotal role in the development and expansion of AI in recent years, enabling thousands of **startups and entrepreneurs** to take AI from research

labs to concrete applications. These investments have accelerated the development of more efficient algorithms, scalable data infrastructures, and increasingly sophisticated autonomous systems, in an environment where technological risk is high and returns are uncertain in the short term. Figure 11 shows the **evolution of venture capital (VC) investment in AI technologies** by industry sector, from 2012 to 2024, based on OECD data from 2025.

Areas such as **government**, **defence**, and **security** have maintained considerably lower levels of investment, indicating a **lower priority for private VC investors in these fields**. The fact that there is investment in digital security and AI computational infrastructure is a positive for defence. This trend is changing, and new VC funds focused on defence have appeared in the EU in the last two years with increasing deal flow in Member States.

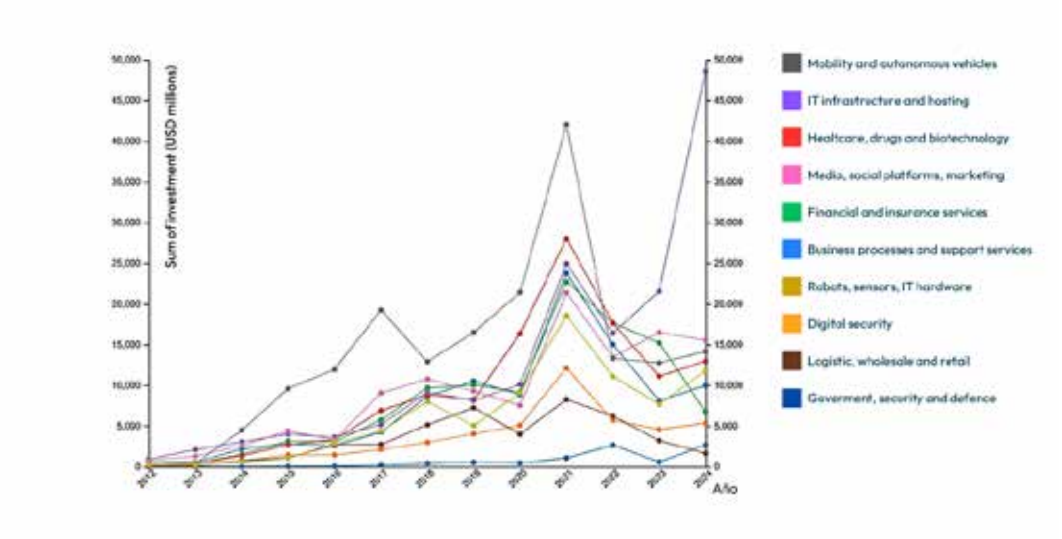


Figure 11. Venture Capital investments in AI. Source: OECD (2025)

AI R&D in Defence in Europe

Collective spending on R&D in the aerospace and defence sectors, financed by both industry and governments, reached an estimated EUR 23,400 million, according to ASD data (2025). Increased allocation of funds to military initiatives (61% vs. 39% for the civilian sector) reflects global trends in the **prioritisation of defence capabilities** and underscores the importance of innovation to maintain a competitive edge and meet evolving challenges.

The **EU's European Defence Fund (EDF)** is an instrument managed and executed by the European Commission, endowed with EUR 8,000 million for the period 2021-2027, of which EUR 2,700 million are directed to research and EUR 5,300 million to defence development. The "**Permanent European Structured Cooperation**" (PESCO) brings together EU countries on a voluntary basis to cooperate in the development of defence capabilities through national funds.

The industry has the support for research and technology from the **European Defence Agency (EDA**). To ensure the identification of technological gaps and areas of common interest for cooperation, the **General Strategic Research Agenda (OSRA),** the EDA's R&D planning tool developed together with its Member States, provides a shared view of the most important technical challenges. Since its creation in 2004, the EDA has managed some 250+ R&D projects, worth more than EUR 1,000 million.

According to a study by the *European Parliament*, the **life cycle of defence equipment** is divided into 10% for R+D, 30-35% for investment (production and procurement), and 55-60% for operation, maintenance, and disposal, as illustrated in Figure 12. Notice that ***EDF*** *(European Defence Fund)* is complemented by the Regulation ***ASAP*** *(Act in Support of Ammunition Production)* and the Regulation ***EDIRPA*** (*European defence industry reinforcement through common procurement act*) to support later stages of the procurement processes.

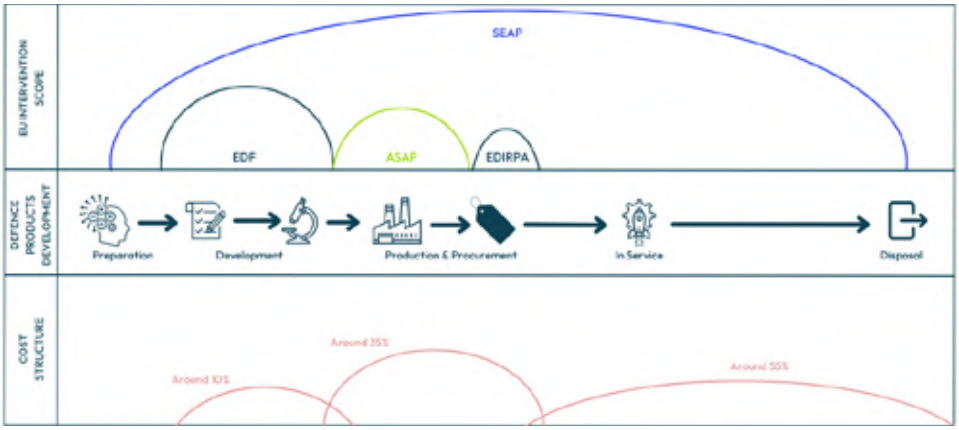


Figure 12. EU tools and frameworks to provide support at crucial stages of the defence equipment lifecycle. Source: European Commission (2024)

Several Spanish companies have been important **beneficiaries of funding from the EDF** in various projects. These companies have participated in projects related to hypersonic defence, cyber resilience, aerospace systems, and naval capabilities, highlighting Spain's strategic role in the European defence industry.

The **SESAR 3 Joint Undertaking** (*SESAR 3 JU*) is a public-private institutional European partnership created to carry out the digital transformation of air traffic in Europe (European Digital Sky). Due to the war in Ukraine, **SESAR** has started activities to integrate civil and military airspace management. In the field of UAS there are technological synergies in AI between SESAR programmes and the military applications of this type of air vehicle.

Finally, the **DIANA (NATO)** programme is noteworthy, with a **network of test centres** in countries of the Atlantic Alliance that will cover the projects approved in different calls. One of them at the **UPM** is related to AI (*Neurotechnology and AI Test Centre*).

In Spain, the main objective of the **COINCIDENTE programme** (*Cooperation in Scientific Research and Development in Strategic Technologies*) is to take advantage of the civilian technologies developed within the scope of the National R&D Plan to incorporate innovative technological solutions of interest to the Ministry of Defence. In 2024 a specific area of AI was added. The participation of universities (40% of R&D projects) is clearly visible, although this presence has decreased in recent years. SMEs are relevant in AI projects, although it seems that in recent years medium and large companies are beginning to appear.

TACTICAL, OPERATIONAL AND STRATEGIC DIMENSION OF THE USE OF AI IN DEFENCE

Three major topics in which AI plays an essential role in defence are discussed: the evolution towards an **intelligent battlefield**, the growing use of AI in the so-called **hybrid and cognitive warfare**, and the importance of AI in a dual domain such as **space**. In all the mentioned topics, the use of AI is evolving rapidly, so attention will be paid to the reasons for its progressive adoption and the existing barriers that could limit its use.

The first of the selected topics, **intelligent battlefield**, focusses on the role that AI plays in having an integrated vision of the situation on the battlefield based on the capture and analysis of data, as a basis for **autonomous or semiautonomous decision-making**. It will focus on the use of command-and-control (C2) systems, the need to manage integrated communications systems at various levels focused on the concept of combat tactic cloud, and on the use of autonomous or semiautonomous weapons and their interaction with manned systems.

The second of the selected topics addresses the role played by AI in the expansion of hybrid and cognitive warfare. It pays special attention to the way in which the use of AI became an essential factor in a gradation of intensity that goes from hybrid threat to hybrid conflict and, finally, to hybrid warfare combining kinetic, cyber, or information control actions. It is also intended to account for the growing use of **AI in cognitive warfare** and, especially, in the importance it has acquired in **disinformation** and **narrative generation** as an essential factor in hybrid and conventional wars whose impact is increasing.

Finally, with the third of the selected topics, the **use of AI in the space defence sector**, the use of AI in an eminently dual domain is addressed, given that many of its platforms (whether individual satellites or forming part of constellations) assume civil and military functions for communications, observation and navigation, regardless of the emergence of specific military payloads and the development of anti-satellite weapons (both hard and soft). Progressively, **space became a fully integrated domain** together with land, sea, air, cyber, and cognitive domains within the framework of the concept of **multi-domain operations** that is configured as a key element of the use of AI in military operations.

Evolution towards an intelligent battlefield

The **introduction of advanced technology systems in the battlefield** to get the superiority against the enemy has been a constant trend in human history. To do so on time and effectively, by adapting military tactics and strategies, if needed, constituted a **key factor for the successful assessment of new technologies over time.**

Within each historical moment, the effort to make available technology-based combat systems able to overcome the defences of the adversary has pressed both conflicting sides to use the most advanced technology, even, when some risks will emerge from its relative lack of maturity. Then, the battlefield behaves as an experimentation laboratory to mature technology systems, and, on some cases, it serves a key role for spreading multiple civil systems out in society. In 2025, **three main features** deserved attention because they have introduced more relevance and complexity:

1. **Faster deployment of technology innovation** in weapons and defence systems on the battlefield compared to previous historical cases.
2. The **growing use of dual technologies**, most of them generated in the civil domain and later on adapted to the military domain to satisfy specific requirements and urgency.
3. The need to deploy automatic support for decision making or for the execution of actions supported by AI algorithms integrated in **very complex interoperable technology systems.**

AI powered systems are deeply changing the way that military operations are conceived and implemented by improving decision making, the situation awareness in the field, and the dynamic allocation of resources. From a technical perspective, main defence areas where AI systems are playing a prominent role are the following ones:

- **Solutions based on the management of large volume of historical and real-time data.** As an example, AI is applied to logistics and predictive maintenance to maximise the use of material resources.
- **Electronic Warfare (EW).** It refers to the use of digital technologies to disrupt or disable the enemy computing systems, communications networks, and infrastructure, through the launching of smart cyberattacks, anticipating threats, and espionage operation.
- **Intelligence, Surveillance, and Recognition (ISR):** It implies the use of sensors, drones, satellites, and other platforms to collect and analyse data on positions and movements of enemy forces. AI-powered systems could analyse a large volume of data and extract conclusions from imprecise data at much higher speed than human operators can do.
- **Computer vision**: It refers to the capture and analysis of visual data from images and videos to detect, recognise and track objects, facial reconnaissance, scene understanding, and automatic elaboration of topographic maps. Relevant information and instructions could be sent to robots, drones or any other autonomous systems.

- **Human-machine interface (HMI):** They allow humans to interact with AI systems by reducing the cognitive load, improving situation awareness and facilitating fast decision making in high stress environments. Among those techniques, natural language processing and inference systems from large language model (LLM) are being used to facilitate a fluid interaction between humans and sophisticated weapon systems.
- **Autonomous systems:** they refer to any type on an unmanned vehicle, drone or robot, to be able to operate without human interaction. Usually, they are designed to perform recognition and surveillance tasks by complementing or substituting humans or integrated into other manned systems.
- **Swarm intelligence**: AI algorithms designed to coordinate the behaviour of multiple autonomous systems that cooperate to achieve a common goal. This area is linked to group intelligence techniques and the way in which individual behaviour contributes to swarm intelligence.
- **Command and control (C2):** It needs AI for data analytics and management on large volumes of data and their visual presentation to human operators.
- **Edge AI**: It implies the use of AI algorithms to real-time processing of data in the Edge of the network (i.e. devices), to reduce latency and improve decision making in applications with autonomous systems and cyber warfare.

The **explosion of generative AI** in recent years with a multitude of applications for end users has also reached the defence sector. The basic question in adopting it in the military environment is to **determine whether generative AI systems can be trusted** in which training depends on the use of data (much of it classified) that cannot be externally verified.

As a result of these **potential risks**, the militaries of major military powers have put in place internal processes of **experimentation and validation of Generative AI techniques** before their widespread adoption. The U.S. Department of Defence (DoD) created a special task force called *"Task Force Lima"* in August 2023 to analyse and evaluate the use of generative AI in national security issues, as well as recommend its responsible use and provide secure implementations in all DoD units.

As an example of these efforts in the US *Scale AI* has developed a **military-specific LLM** called ***Defence Llama*** built on top of Meta's *Llama 3* to be able to answer defence-related questions and scenarios. Recently, the US Department of Defence launched a generative AI platform called the "*Army Enterprise Large Language Model Workspace*" to streamline communication, improve operational efficiency, and drive innovation. A further step in the direction of real AI adoption is the "*Thunderforge*" programme whose goal is to provide a unified planning ecosystem in which AI agents simulate war games and plan scenarios.

All these efforts announce, if the results of these projects are as expected, an **acceleration in the use of military systems based on AI agents supported by generative AI**

techniques in various areas of planning and decision-making as a complement to the human decision maker.

AI in the multi-domain vision

The **explosion in the development and deployment of low-cost fixed or mobile aerial, terrestrial or maritime ground sensors** that capture detailed information from the terrain combined with their automated processing in real time to feed decision making and their interaction with robotic systems is accelerating a process of **disruptive change on the battlefield.**

These elements gradually lead to the existence of a **"transparent" battlefield** in which the concealment of movements of troops or military equipment on a medium or large scale for prolonged periods of time is not possible. "*Transparency*" on the battlefield refers to an adversary's ability to obtain detailed, near-real-time information about enemy activities and movements by combining information from communications, intelligence, and surveillance capabilities. As a result, the combat tactics employed have evolved in a short time in response to the need to **increase mobility with light and self-sufficient units**.

Information to be considered by a military decision system is very voluminous and changes rapidly with the deployment of a multitude of sensors. For this reason, data interpretation is very difficult, exclusively by human operators. Some **trends in the use of AI** can be identified:

- Increased **use of AI in the automatic identification and selection of targets** based on the integration and analysis of historical and other data obtained in real time from multiple sensors.
- Introduction of **AI algorithms in decision support platforms** both at a personal level (in the form of an automated assistant) and in **command-and-control systems** at different organisational levels.
- Use of **lethal isolated or swarm autonomous or semiautonomous weapons systems** with varying degrees of intelligence.
- Embeddedness of Intelligent **Electronic Warfare Systems** in multiple military systems.

Intelligent weapon systems

In just a few years, **multiple smart weapons systems or autonomous weapons systems with various AI-based solutions have been incorporated**, together with microelectronic systems, sensors, and actuators of all kinds, in a technological race in search of supremacy between great powers. The basic idea is to **delegate decision-making to AI algorithms** partially or fully (i.e., with or without human operator intervention) **to speed up the decision process** and be able to handle huge volumes of data that a human operator would not be able to analyse.

This is a **progressive approach**. Starting at the level where the computer system has no function and it is the human operator who makes all the decisions, to the maximum level where it is the AI-powered system that makes the decisions and the human none, there are **many intermediate levels which imply progressively accepting greater responsibility for the algorithms of the computer system**, allowing approval, temporary veto, or providing the information in time to the human operator for the taking of alternative measures to undo the action initiated. In all these cases, can be said that "*the human is in the loop*".

Finally, the **higher levels of automation** correspond to the use of algorithms that make the decision. Humans may or may not be informed of it, depending on the level considered, but it is outside the decision loop. Another category that is much more widely used today is **semi-autonomous weapons systems**. The basic difference is that with fully autonomous weapons, the decision is made only by the AI algorithms incorporated into the system, once the target has been trained and defined, and in semi-autonomous systems a human operator gives the final order to attack or not to attack an identified target.

Autonomous systems used as weapons which can derive in severe impacts on persons are called ***Lethal Autonomous Weapon Systems (LAWS)*** by the United Nations. A common definition is *"weapons systems that use artificial intelligence (AI) to identify, select, and engage targets without human intervention."* In recent years, countries such as the United States, the United Kingdom, India, Israel, Iran, South Korea, Russia, and Turkey have invested heavily in integrating AI into LAWS development. Currently, **armies around the world use more than 130 weapons systems that can autonomously track and attack their targets**.

As an example of these capabilities, **advanced drones** are often launched in *capsules* from far away; once released, they can fly short distances and attack without human input. Improvements in camera technology and AI make it possible for these drones to identify and focus on specific targets used in their training process. To address those challenges, **Replicator**, a new US military programme is based on LLM models for both kamikaze drones and anti-drone defences focused on creating systems to respond quickly to drones attack, and countermeasures to kamikaze drones. As a relevant shift of common practices, *Replicator* programme relies heavily (75%) on innovative start-ups and suppliers that do not participate in the usual defence supply chains, looking for the fast introduction of radical innovations.

The **technological evolution towards "smart drone swarms"** based on hundreds or thousands of air-based, terrestrial or maritime drones in which each of them can identify targets in real time and communicate with their neighbouring drones will mean a qualitative change with effects on military tactics. Success in the mission of a swarm of drones requires integrating the capabilities of individual drones to achieve **collective behaviour**. Three **basic approaches to swarm coordination** can be established:

- **Centralised approach**. All interactions are made with the operator who receives information from the individual drones, decides, and sends orders to each of them. There is no communication between the drones.
- **Decentralised, semi-autonomous approach**. The human operator communicates with a drone for the reception and transmission of data and orders, and this *master drone* communicates with the rest of the swarm members. Some lower-level derivative actions could be performed autonomously by individual drones.
- **Fully autonomous decentralised approach**. There is no human operator. Each drone exchanges information with all or some of the nearby drones to decide on the next moves and actions following behaviours for which their AI algorithms have been trained. This approach could support heterogenous swarms where drones could differ in size and capabilities.

All the major world powers are working on the **development of drone swarms for military purposes**. This technology is not only in the hands of great technological powers. Some **European companies** with innovative approaches for swarm control can be mentioned (not exhaustive list): *Saker* (Ukraine), *Quantum Systems* (Germany), *Thales* (France), Helsing (Germany), *BlueBear AI* (UK), *Swarming Technologies & Solutions* (Spain).

The announcement made in July 2024 by the Ukrainian army of the use on the *Kharkiv* front, for the first time, of a **combined attack of aerial drones and ground vehicles, managing to capture Russian troops without direct human intervention**, is, from a technological point of view, an example of the speed with which new combat tactics are being adopted with swarms of remotely piloted heterogeneous autonomous vehicles. **The evolution towards the intelligent battlefield is accelerating.**

These innovations represent remarkable advances in drone technology, but **technological revolutions in military affairs require more than the widespread adoption of new technologies**: armies must develop new operational concepts, integrate new capabilities into broader military systems, and adapt their organisational culture and structure; all of this requires accumulating experience.

Relevance of AI in Hybrid and Cognitive Warfare

The role and relevance of AI have grown in **asymmetrical conflicts** and, especially, in the so-called "**hybrid war**". A distinction can be made between **three types of "hybrid" situations** (threat, conflict, and war) that allude to a gradation in intensity and in the social impact and military involvement that they entail:

- H***ybrid threat***: A phenomenon resulting from the interconnection of different elements that, together, constitute a more complex and multidimensional threat to societies.

- ***Hybrid conflict***: A situation in which the parties refrain from the open use of (armed) force and act by combining military intimidation (without reaching the threshold of a conventional attack) and the exploitation of economic, political, technological, and diplomatic vulnerabilities through planned and synchronised actions.
- ***Hybrid war***: A situation in which a country resorts to the open use of (armed) force against another country or against a non-state actor, together with the use of other means of coercion (e.g. economic, political or diplomatic) combined with covert or non-covert operations of lesser intensity.

A factor of success is the **synchronisation and escalation of actions**, both from a perspective of *horizontal escalation* between different domains of power (military, political, economic, civil, or information) and *vertical escalation* with different levels of intensity and visibility of the hybrid action in the population.

Figure 13 shows various tools of power on which hybrid warfare actions must be synchronised: **military**, **political**, **economic**, **civil**, and **information**.

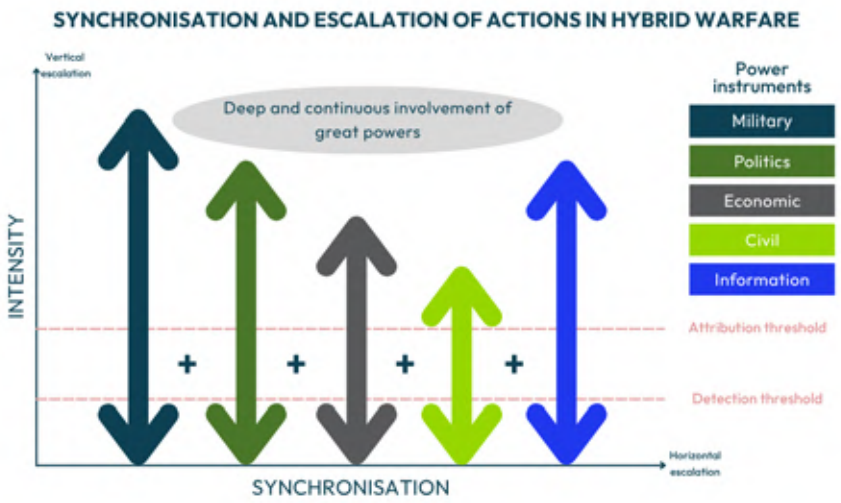


Figure 13. Synchronization and escalation of actions in hybrid warfare. Source: adapted from https://assets.publishing.service.gov.uk/media/5a8228a540f0b62305b92caa/dar_mcdc_hybrid_warfare.pdf

Two **relevant visibility thresholds** are useful to understand the conflict:

- ***Detection threshold***: minimum level of intensity of hybrid action that allows a government to detect that a hybrid threat, conflict, or war is occurring.
- ***Attribution threshold***: minimum level of intensity that allows convincing attribution (once detected) who is the actor that causes it to be able to carry out actions with solidity and not refutable.

Hybrid warfare develops as a temporary process in which the level of escalation (increase in the intensity of the conflict) fluctuates, is not linear, and is punctuated by various "crises" and "destabilisation" actions over time. This grade depends on a strategic decision on the level of confrontation that is desired to be achieved with these actions in response to the impact obtained and the potential response of the adversary. Then, both attribution and detection thresholds evolve over time.

For the *Hybrid-CoE Centre of Excellence*, **technology is one of the main drivers** of hybrid warfare and hybrid warfare theories. A *Hybrid-CoE* analysis identified three types of technologies.

- Technologies that target manipulating radio access to information using **electronic warfare techniques** to jam the radio signal, spoof, or other cyberattacks.
- Technologies oriented to the **manipulation of information and its narrative** by acting on the services offered by digital platforms generating "disinformation" through the generation of false or tendentious news.
- **Emerging technologies** such as neurotechnologies, autonomous systems, extended reality or, in the future, interacting with quantum technologies.

The potential **impact of hybrid attacks is accelerated by the use of automated systems** due to the use of AI systems capable of analysing multiple contextual data in such a volume that it is impossible for human analysts to use it. With the use of AI, we enter an area of **explosion of the capacity for "cognitive warfare", superimposed on actions of a hybrid nature** (see figure 14) whose objective is the **mastery of information for the construction and dissemination of narratives aimed at achieving political objectives**.

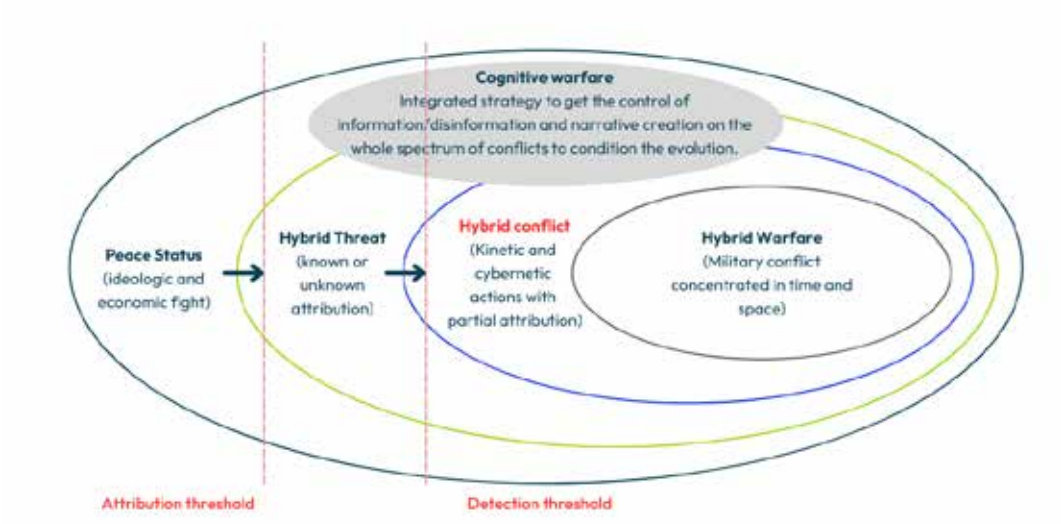


Figure 14. Threats, conflicts and hybrid warfare, and cognitive warfare. Source: own elaboration

It would not have been possible to achieve the impact of cognitive warfare in the current situation without the **use of social networks as a "weapon"**, and the (automated) launch of sophisticated cyberattacks with the help of AI tools (e.g., through the automatic generation of personalised multimedia messages with empathetic bots, distortion of reality, and their massive dissemination in target population groups). However, the way in which it is addressed depends on the country considered, as the cases of Russia and China has shown.

- **Rusia** complements the warfare in Ukraine with cyberattacks and disinformation campaigns against EU targets. Therefore, the EU reinforced in 2024 the sanctions over persons and entities participating in Russia backed actions against the EU.
- In **China**, cognitive warfare adopts the term "*algorithmic cognitive warfare*". The goal is to get the most out of the combination of data analysis algorithms and social media recommendations to effectively influence an individual's behaviour. It leverages the vast amounts of data available on the behaviour of people and entities to train AI algorithms.

A **cognitive warfare model** should be focused on the cognition to which physical performances in the field are subordinated and, on the information side, linked to the **dissemination of narratives** in the cognitive domain at the national and international level. To address it systemically, **five types of instrumental dimensions** are used:

- Tools that exploit cognitive biases and perception.
- Tools related to neuroscience and biology.
- Tools that exploit social psychology and group dynamics.
- Tools that employ techno-social applications.
- Information technology tools.

A basic element to implement cognitive warfare is the **mastery of disinformation campaigns**. Its success depends on three conditions: **narratives** that effectively and persuasively convey the message designed for a specific objective; **dissemination** of the message to a target audience to influence policy decisions at the national or institutional level; and **persuade** a sufficient proportion of people of the veracity and relevance of the message to generate a chain of reactions that achieve the objective.

The increase in disinformation, supported and enhanced by the development of AI, has penetrated governments, institutions, and citizens with a destabilising effect. The *General Assembly of the United Nations* has expressed concern about the proliferation of disinformation and needs to promote international cooperation in the fight against disinformation.

Currently, to pursue the dominance of **AI-powered digital platforms** is part of the strategies of the great technological powers to **influence public opinion** around the world; above all, taking advantage of the enormous dissemination and use of **social networks** and the impact of the opinion of certain entities and people. From the point of view of political

interest, the processing of this personal information also makes it possible to analyse or introduce biases towards certain ideologies, political parties, members of the government, representatives, or candidates in political elections.

Furthermore, **specialised AI tools have made it possible to automatically create disinformation campaigns with synthetic realities** that are difficult to counteract. Multimodal generative AI (cloning not only the image, but also the voice and body language in hyper realistic videos) is combined with other types of tools such as **virtual reality** (with the generation of realistic 3D models) to enable cognitive attacks based on a growing area such as emotional manipulation by taking advantage of virtual reality environments that have proven their ability to induce negative emotions. The use of AI tools offers improvements to different actors involved in cognitive warfare to achieve the desired effect. In detail:

- Content that is published and shared can be analysed using artificial intelligence (AI) techniques such as **natural language processing (NLP).**
- Various classification tools, such as decision forests and LSTM neural networks, facilitate **machine translation**.
- **Graph technology** harnesses the potential of AI to analyse relationships between data points.
- **Machine learning systems** can create tools to detect images that have been manipulated or manipulated, for example, by looking for traces left by systems used to capture altered images.
- AI applications can also be trained to **detect misinformation on social networks** and issue warnings. By analysing blocks of data from exchanges on networks such as Twitter and Telegram, AIs can recognise stylistic elements typical of fake news.
- They can also be trained to **identify potentially problematic content** and help operators understand why it has been flagged.

Being fully aware of the severity of this situation, the **EU strategy** is based on strengthening a **comprehensive resilience ecosystem against hybrid warfare** involving coordination and exchange of information between different types of actors. It is based on the ***Rapid Alert System*** (SAR) which aims to develop a comprehensive framework and methodology for the systematic collection of incidents facilitated by the *Information Analysis and Exchange Centre* (FIMI ISAC) that increases the resilience of Europe to external interference.

In the context of cognitive warfare, **cognitive abilities** of humans are the most relevant. For this reason, **neurotechnology as a dual use technology** has aroused interest from defence research agencies to converge with AI in a disruptive step forward.

The cognitive improvement of human beings affects the collection, analysis, and use of brain activity data, on which AI algorithms play a relevant role. **Improved cognitive performance can be "trained**." The technological evolution of **external prostheses,** such as brain monitoring and stimulation helmets equipped with sensors that allow information on brain

activity to be obtained, or **internal prostheses** such as brain implants, can also be used. Further back in time, **cognitive improvements based on gene therapies** using techniques such as *CRISPR* are being considered and could represent a leap forward in the future.

In that context, a new generation of **cognitive weapons** will progressively be available to large powers. **Probably, next decade will see the deployment of some of them. Neuroweapons** refer to technologies used to enhance or damage the cognitive and/or physical abilities of a combatant or target or otherwise attack individuals or critical infrastructure in society. The intended goal is to **alter a soldier's behaviour** by influencing attention, decision-making, and reaction. Having **miliary personnel with increased physical and mental performance** will allow **cognitive warfare** to be extended to the battlefield of social networks.

AI in the defence space sector

The **dominance and exploitation of the space sector** has become a decisive factor from the perspective of defence. A key element in understanding the geopolitical relevance achieved by the space sector is because **space technology has a dual character**, historically linked to confrontation between great powers, with the involvement of the Armed Forces and the defence industry. As a relevant fact, 70% of the satellites orbiting the Earth in 2023 were military or dual use. In 2023 alone, 107 military satellites were launched, bringing the total number to more than 900 and an estimated 2,500 military satellites in the next ten years.

Figure 15 identifies the **major drivers of AI use in space**. In the central part, two meta-drivers have been indicated linked to the need to **reduce the cost and development time** of a satellite or other space object and, at the same time, maintain maximum confidence in the processes of **verification and validation of space components and subsystems**.

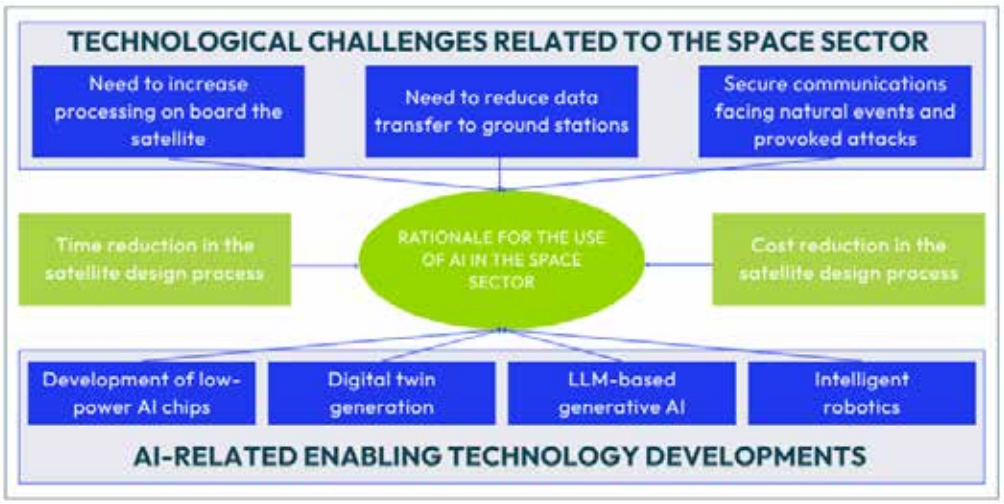


Figure 15. Drivers of the use of AI in space. Source: own elaboration.

Three **technological challenges** are indicated at the top of the figure:

- **Increase processing capabilities** on board the satellite or spacecraft for smarter space systems for platform and payload management
- **Reduce the transfer of captured data to ground stations** with the aim of reducing reliance on satellite links and the window of visibility towards terrestrial stations.
- **Protect communication systems against cyberattacks** caused to disable the operation of the satellite.

At the bottom of the figure, four **technological developments related to AI** are identified as "enablers" in the face of the challenges indicated:

- Development of high-performance, low-power, and space-adapted **chips for AI model (re)training and inference extraction**
- Generation of **cyber physical digital twins** to accelerate the rapid design of space systems based on an accurate digital model of the system to be developed.
- Use of **generative AI tools** based on the use of large language models (LLMs) adapted to the needs of space and defence.
- Use of **intelligent robotics** in space based on robotic arms or autonomous robots.

These areas of technology provided the bases for the application of AI in the space defence sector. The most relevant are:

1. **Improved spatial domain awareness (SDA).** Understand and manage space assets located in space and their actual position to identify nearby objects, derived threats, and reduce operational risks.
2. **Defence of satellite navigation**. To implement methods that allow knowing if the GNSS navigation signal is altered or impossible to obtain, offering alternative navigation techniques so as not to depend on the satellite signal.
3. **Intelligent analysis of satellite images**. Processing AI-powered images taken by the satellite, either on the satellite itself or at ground stations to identify specific objects of interest, and feed decision-making on specific platforms
4. **Automatic orbit adjustments to avoid collisions**. Knowledge of the distance and orbit settings of satellites from earth stations or by the satellite itself if it has sufficient sensors and processing capacity to avoid impacts with other objects in space (e.g. space debris or asteroids).
5. **Predictive maintenance of satellites**. Use of AI algorithms to plan satellite maintenance processes based on time-series analysis of data combined with other data captured in real-time
6. **Optimization of military space communications**. Use of AI to achieve robust broadband communications, immune to natural or man-made interference in the space environment.

7. **Space cybersecurity**. Cyber-attack defence systems of data to or from satellites, whether data generated by on-board payloads (e.g. images) or control signals as part of navigation or communications networks.
8. **Intelligent space robotics**. Fixed autonomous robots (e.g. robotic arms) or mobile robots (e.g. anthropomorphic or not cooperating with humans, space exploitation vehicles) to perform multiple missions without human intervention.
9. **Common frameworks for the simulation and interoperability of spatial data**. Ensure the interoperability of spatial data to share data between allied armed forces and have multi-source and multi-vendor systems and applications.
10. **Integration of AI with quantum technologies**. Analysis of the way that AI could be integrated with the use of quantum technologies (communications, sensors, or computing) in space applications.

This list of **AI-based space applications is changing very fast** by exploiting more powerful on-board processors and lighter versions of LLM systems.

ETHICAL AND REGULATORY DIMENSION OF AI IN DEFENSE

The objective of **military ethics** is to determine the criteria and conditions that make war, accepting violence as an essential component of its nature, and assuming the use of force with lethal effects on people, legitimate in its initiation, development, and consequences. This issue has gained **relevance with the use of AI in decision making and the role that humans can play**. AI-based systems have demonstrated their ability to help humans improve their activity through so-called ***"intelligent agents"*** that take on functions that until recently were carried out only by human beings. The use of ***military intelligence agents*** is being experimented with. Intelligent agents can be part of **lethal autonomous weapons systems (LAWS)** or as an enhancement to other conventional weapons.

The United Nations' position since 2018 has been that **LAWS** are "*politically unacceptable and morally repugnant*" and has therefore called for them to be banned under international law. In the *General Assembly Resolution* of 24 December 2024, an area on ***"Artificial intelligence in the military field and its consequences for international peace and security"*** was included. China proposed in 2022 the need to distinguish between "*acceptable and unacceptable autonomous weapons systems*"; anyway, **consensus is not available yet**.

AI must be addressed with a **balanced ethical and regulatory framework**. Figure 16 shows all the elements involved. In the absence of a specific legal framework, the treatment of AI in the military field is **subordinated to international law**.

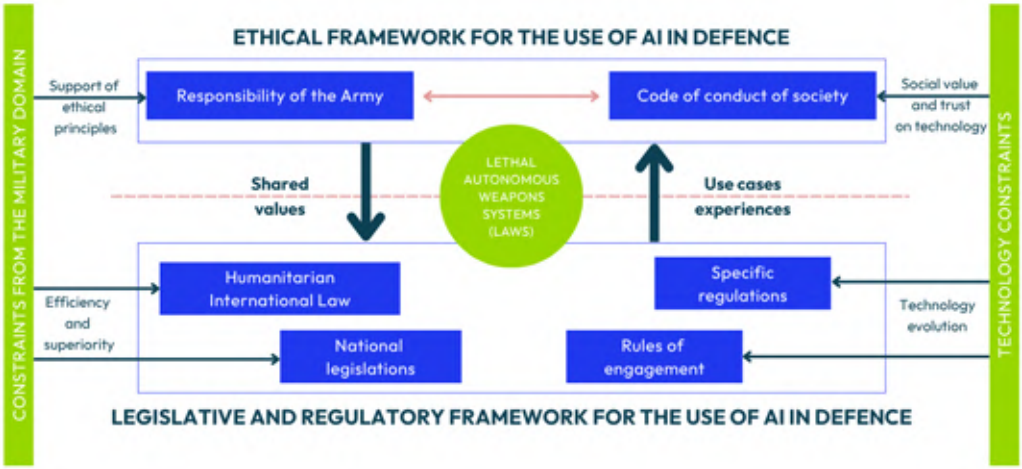


Figure 16. Relations between the ethical and regulatory framework. Source: own elaboration

The *Summits* celebrated between states (in 2023 in the Netherlands, in 2024 in South Korea, and the next one planned in 2025 in Spain) called **Responsible AI in the Military (REAIM) aim to establish ethical limits to the military use of AI**. They do not imply the creation of a legislative framework, but the agreements on "voluntary" actions based on discussion and experience through the implementation of an **action plan**. However, there is no guarantee that, in the event of an acute military conflict, they will be followed by the contenders when survival is at stake.

The EU AI Regulation published on 13 June 2024 is not applicable because it explicitly excludes national security, defence, and military purposes. In fact, during the negotiations, some member states pushed for exemptions to preserve Europe's strategic autonomy, ensuring minimal restrictions on AI in defence and security. The Regulation introduces a **risk-based classification for AI applications**, imposing compliance obligations on suppliers that could be transferred to the military domain. However, the **European Parliament** has consistently urged the Council to prevent the development and use of LAWS that operate without meaningful human control and to push for them to be banned worldwide. It highlights the **importance of ethical guidelines, transparency, and accountability in the deployment of AI, especially in areas affecting military operations.**

Looking to the future, the **convergence between AI and neurotechnology** has generated a new framework for ethical and regulatory discussions on the development and use of cognitive and social augmentation technologies. There are two main **ethical concerns**: **mental privacy** and **human agency**. Even if today cognitive technology is not mature enough to control mental privacy and human agency, it is evolving very fast.

- **"Mental privacy"** refers to the acceptance that the contents of a person's mind are only consciously known by that person. With the available technological, it is not possible to access that content, unless the person decides to share it with others by talking, writing, drawing or using body language to express it and communicate it to others.
- **"Human agency"** refers to a person's freedom and autonomy. Neurotechnology in combination with drugs can be used to influence your behavior, thoughts, emotions, or memories, by increasing or inhibiting some brain abilities

The **relationship between these two ethical concerns and the neuroweapons** mentioned in the previous chapter around *Hybrid War* is evident, so their relevance will be growing.

EU TECHNOLOGICAL SOVEREIGNTY IN AI FOR DEFENCE

Levels of technology sovereignty

At a time when the EU wants to increase its strategic autonomy to be able to make its own decisions without depending on others as much as possible, knowing the level of technological sovereignty achievable from a realistic position is a basic element. **Analysis of technological sovereignty** can be done using a model such as the one shown in Figure 17 which represents the degree of technological self-sufficiency achievable (from 0 to 100%) in various areas of political intervention at three different levels.

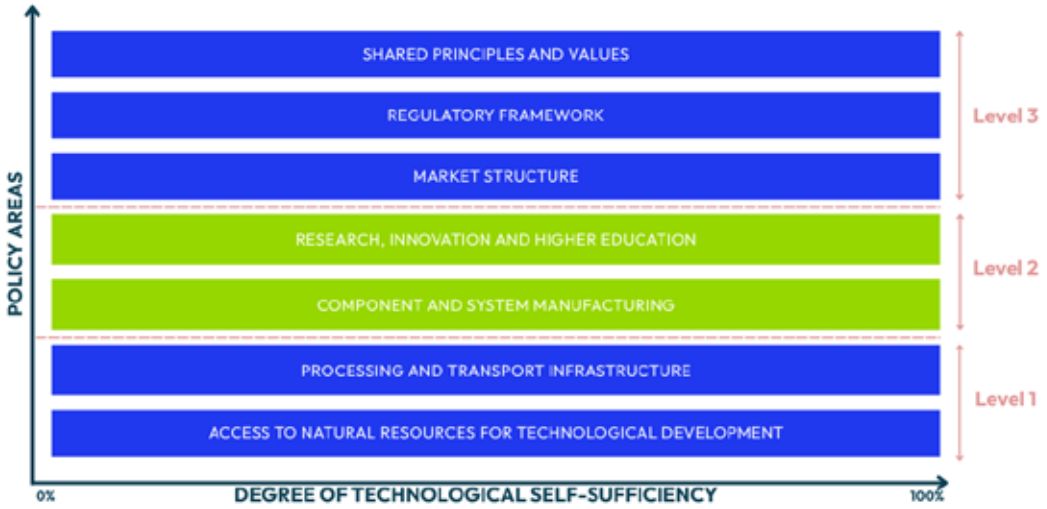


Figure 17. Levels of technological sovereignty. Source: Own elaboration.

The **first level** relates to the access to natural resources and infrastructures for processing and transporting materials. The **second level** relates to research and innovation capacities

and trained human resources, as well as to the manufacturing of industrial components and systems. Finally, the **third level** is related to the structure of the market, the regulatory framework, and the shared principles and values. From a qualitative perspective developed by the Working Group, figure 18 exemplifies the EU's situation of technological sovereignty in relation to AI.

- **Access to natural resources** in the EU is conditioned by the need to manufacture semiconductors used in AI, and the energy costs to power the data centres used in the training of AI algorithms or for the extraction of inferences. In both areas, the EU has a weak position.

- The **infrastructures for processing and transporting** the raw materials or components necessary for the development and use of AI systems oblige the EU to ensure supply from distant countries, mitigated by diversifying suppliers in friendly countries or bringing them physically closer to the EU. The weakness of the EU in having large transatlantic subsea fibre optic cables owned by non-European companies also plays a role in the EU weak position at this level.

- The **manufacture of AI components and systems** is conditioned in the EU by the lack of large foundries for the manufacture of AI chips, although it is good at developing extreme photolithography (EUV) machines capable of manufacturing AI chips. It is also necessary to improve technological sovereignty in **supercomputers and large data centres for AI**.

- The **research, innovation and training of human resources** in AI activities already carried out by the EU are remarkable. However, it must increase efforts to train more human resources in AI technologies, retain them, and exploit opportunities to attract researchers from other countries.

- The **structure of the European AI market** presents a heavy dependence on large non-European AI companies and platforms offering AI products and services in the cloud, with few highly valued AI startups in the EU.

- The **EU's regulatory situation in AI** has two weaknesses: 1) the need to reconcile regulation and innovation under the same or better conditions than those existing in other countries and 2) the need for regulation to evolve with AI technology.

- A key element of the regulation and evolution of the market is the **set of shared principles and values in relation to AI** with which the EU wishes to see itself reflected in the world.

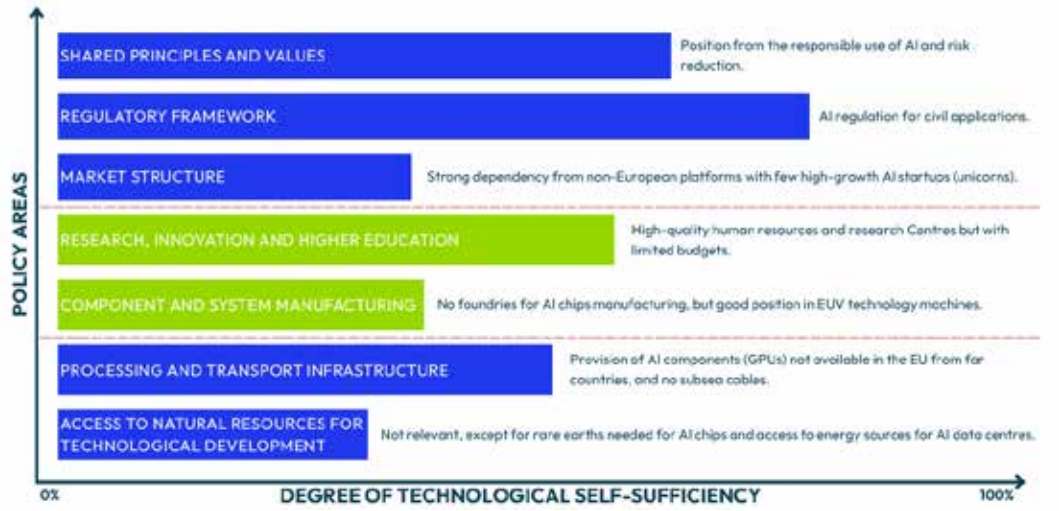


Figure 18. Assessment of the EU's technological sovereignty in AI. Source: own elaboration

Figure 19 provides an overview of the **technical layers of AI system development** (*stack model*) and potential impacts on defence applications.

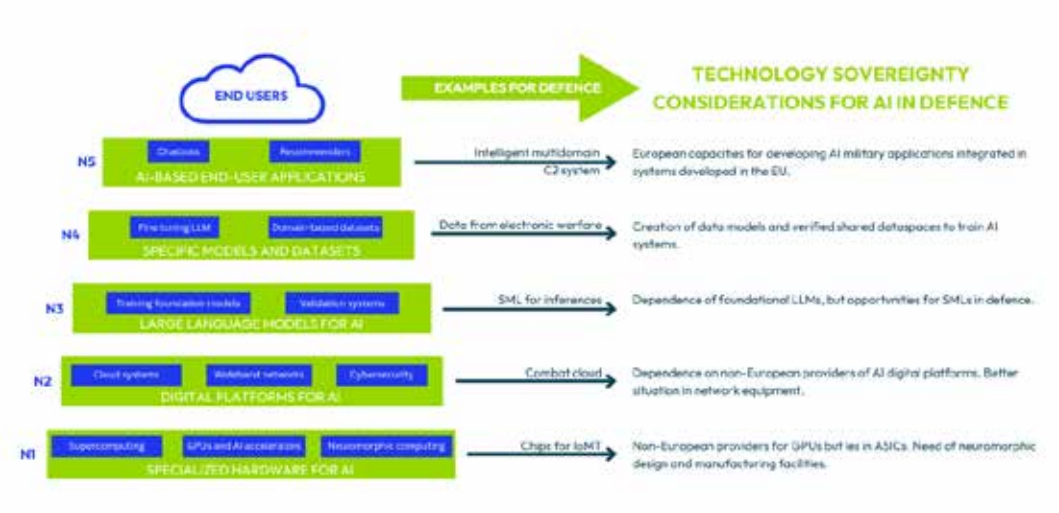


Figure 19. AI technology sovereignty considerations in defense in a layered model. Source: own elaboration

Since **semiconductor technology is dual**, there is nothing to prevent the previously indicated efforts to improve technological sovereignty in semiconductors from benefiting their application in defence, including **AI-designed chips such as GPUs and inference accelerators**. However, there are two relevant aspects that influence decision making: a **limited market volume** in terms of the number of chips that is much smaller and **cost considerations that**

are less relevant than those that apply for civilian applications with AI chips embedded in millions of products (as AI-powered smart phones).

To improve technological sovereignty in AI, the *European Commission* proposed in April 2025 an ***Action Plan*** based on actions on computing infrastructure, data, training, algorithm development and adoption, and regulatory simplification of interest. This action plan affects the European defence industry, which should concentrate on military equipment incorporating AI with a view to its development in the EU member states and, if possible, with common development and procurement models.

Geopolitics and Digital Platforms for AI

The EU must try in the coming years to adopt **European alternatives** ranging from the development of classical semiconductor devices to neuromorphic computing devices, for the execution of AI algorithms, the development of European LLMs, the availability of decision-making platforms, and their integration into multiple military systems.

The **increase of EU resources allocated to the defence industry**, as well as a greater effort toward dual technologies such as AI, can serve as a basis for conditioning Member States to buy European systems and platforms. The European industry should consider a strategy to access a dual market that is global; only way to recover the investment.

By 2030, the **synergies of AI with other emerging enabling technologies**, including *quantum technologies* and *neurotechnology*, open a wide range of possibilities that the EU should be ready to take advantage of now to ensure a sufficient level of EU technological sovereignty in a highly relevant emerging dual use field.

CONCLUSIONS AND RECOMMENDATIONS

A set of the **most relevant conclusions on the use of AI in defence** have been drawn from the report. Based on them, a set of **recommendations for action** is proposed to improve the EU's positioning in the use of AI in the field of defence and its possible transfer to the situation of Spanish defence and its improvement in the coming years.

Making the proposed recommendations a reality in the field of defence is a complex process that requires **political will**, **continuous investments over time**, and the **participation of all actors** at different levels of society from the defence industry to the armed forces of the Member States and the universities and research centres to carry it out.

Conclusions

On the scientific and technological dimension of AI

The following conclusions reflect the **current advances or barriers in the technological development of AI** and its evolution throughout the current decade that have or will have greater relevance in the defence sector.

1. With the development of AI, **a new phase of the digitisation process** has been entered that complements, develops, and builds on the previous phases since the last decades of the twentieth century with a growing impact on society.

   This is an **accelerated and continuous process of digitalisation** that also affects the defence sector, both for companies that generate products and services for military use in the development and manufacturing processes and for their final use by the armies themselves in the exercise of their missions.

2. The **path towards achieving general AI** is not assumed to be a certain fact in the medium or long term with significant differences in experts' opinions on whether it will be possible or not.

   Achieving an **AI that surpasses humans in all facets would require disruptive advances**, not foreseeable at this time. What is possible are multiple and continuous incremental improvements of narrow AI systems focused on many types of problems; in many of them, they already exceed the performance of the average human being.

3. AI acts as a **dual character enabling technology** across socioeconomic domains with cross-inputs, but where the volume of investments and size of the civilian sector are acting as a key driver.

   The main driver of the S&T development of AI in the last two decades lies in the investments made in the civil sector by public and private entities. However, in the defence sector, the starting point is the adaptation of a product or service in the civilian market for use in the defence sector or vice versa to take advantage of the effort made.

4. The progressive **integration of AI algorithms** to provide key functionalities of almost all products and services used by the armed forces will make their use in defence **more transparent to the end user.**

   Integration of AI into military systems makes the end user less aware of its implications. Then training of military personnel and the establishment of clear rules and procedures for use should be a prerequisite for their adoption.

5. The need for massive amounts of statistically **significant, specific data for the training of found**ational models has become an essential factor given the direct relationship between data quality and the validity of results, as well as between the amount of training data and the computational needs that must be covered by specialised hardware.

   This factor affects **machine learning (ML) techniques** such as deep learning (DL), including generative AI based on supervised learning. **Reinforcement learning** can only be applied in highly controlled environments, which makes them unusable in combat situations, although they are valid for training.

6. **Multi-agent systems**, made up of multiple AI agents coordinated with each other by approaching real problems orientated to supporting human beings for the development of complex functions, will accelerate and extend the use of AI in society by approaching the resolution of real problems with significant advantages derived from its use.

   Its use involves the **accelerated deployment of AI agents at all operational levels**, which implies the modification of many of the tactical and strategic processes currently used and explains the apparent delay in its adoption compared to civilian areas.

7. **The growing importance of AI hardware,** both for the development of intelligent sensors and their interconnectivity in military Internet of Things networks and in the training of generative AI models and the generation of inferences, has become a key controlling factor in the current geopolitical and technological battle.

   Need for industry to have the necessary knowledge to develop **advanced integrated circuits and sensors** or stable agreements through reliable suppliers in other countries outside the EU, and for the Armed Forces the ability to adopt it.

8. The manufacture of the most advanced models of **graphics processing units (GPUs)** has become a critical factor in generative AI; Its availability emerges as a **potential bottleneck** and is linked to multiple restrictions and conditions to export them for certain countries.

   Continuous and incremental **improvements in the performance of AI algorithms on specialized chips** (GPUs, FPGAs and ASICs). By the end of the decade, powerful **neuromorphic chips** with much lower power will be available, adapted to the execution of neural network algorithms.

9. **Multimodal generative AI** has matured very quickly, being able to generate information from data, text, voice, image, or video that is very difficult to distinguish from reality, a fact that generates misinformation and difficulties in its management and use that are critical in areas of security and defence application.

The use of **multimodal generative AI has grown in the case of hybrid warfare and cognitive warfare**. This use occurs in a context of high growth in cyberattacks and the launch of disinformation campaigns provoked by state or parastatal actors.

10. Relevant technical problems persist in the use of AI systems derived from the **"black box" problem of algorithms, biases, and "hallucinations"** in the inference processes of generative AI in applications derived from the use of large language models (LLMs), which makes their use in defence applications difficult.

    Both problems represent a barrier to their use in defence that **must be evaluated before their adoption in critical decision systems** in which it is necessary to know the reasons that lead to a certain response of the system; especially in those with potential lethal consequences.

11. The **need to reduce the energy and computational consumption** necessary for the training and calculation of inferences has motivated and accelerated current advances to have (smaller) and efficient language models for use in specific domains, such as some of a dual nature or with contextual constraints such as space.

    The **proliferation of small-language models *(SLM)*** offers opportunities for training with data of military interest. This process also involves reducing the computational and energy needs of data processing centres related to the training of AI models or for the execution of pre-trained algorithms on user end devices.

12. The **integration of AI with neurotechnology is still in its infancy** as it is an immature technology, but it will occur with potential disruptions in society over the next decade and with increasing application in defence.

    The convergence of AI with neurotechnology has advanced considerably in the current decade, although **its use outside the medical field is still limited**. The potential to facilitate the increase of human cognitive abilities and its application to healthy people gives it potential relevance in the field of defence, in which all technological powers are already working.

13. The integration of **AI-based products and services with other technologies such as quantum technologies** will form the basis for the next wave of technological disruptions.

    Given that some of the technologies potentially involved are not mature, it will be necessary to have experimental programmes that allow their potential usefulness to be assessed and, through them, accelerate the maturation process of emerging multitechnological dual products. This integration combined with AI is part of the future **"intelligent quantum war".**

Conclusions on the socio-economic dimension of AI

1. The **global AI market** continues to grow at a very CAGR; especially in areas such as machine learning, generative AI, and intelligent agent systems.

   The dominance of AI and its convergence with other emerging technologies is part of the battle for technological supremacy between the great powers. These growth rates are becoming higher in the defence sector, and they accelerate in the future.

2. The **leadership in the development and use of AI** with global influence on the western economy remains in the hands of the United States, both in terms of market volume achieved and in terms of the stock market valuation of its large digital companies at all links of the value chain.

   In sectors where duality is a key factor, it is likely that **a fragmentation of the AI market** will be consolidated into **blocks or areas of influence of the great powers**, and even of the data spaces used for the training of models.

3. In a very short time, **China became one of the leading countries in the S&T development of AI**, whether measured in the percentage of patents, in the growth of scientific publications, or in the volume of the market reached, which, together, implies the gradual reduction of the gap with the United States.

   China has caught up with the United States in several areas of AI, such as **image recognition** and the development of **efficient language models**, supported by the emergence of multiple startups with disruptive approaches financed by government funds. The potential dual use of practically all generated products is aligned with the concept of military-civilian fusion that China has been advocating for years.

4. The **sanctions and restrictions imposed on China by the United States** for the export of semiconductor or integrated circuit manufacturing equipment used in the training of large language models or for the generation of inferences have boosted and accelerated the development of AI technology in China.

   In response to the imposition of sanctions on the export and import of technological products, **the development of in-house capacities has been stimulated**. Chinese companies have managed to obtain very appreciable results in mobile communications, LLM training or weapons systems without the need to use the most powerful versions of AI chips.

5. **Defence companies have embraced the dual nature of AI** and are accelerating its inclusion in a multitude of military products by collaborating with digital companies, adapting civilian products, and competing with companies in the rest of the world.

European companies are following the same trend, although growing slowly, and maintaining dependence on AI components and subsystems with other countries, which has led to a rethink of the EU's strategic alliance framework with the aim of improving the resilience of its AI supply chain and the generation of its own capabilities.

6. **The adoption of AI in the defence sector is beginning to spread** not only by large digital companies that take advantage of the duality of use for their integration into digital products and services, but also by the role played by a multitude of highly specialised start-up companies.

   The emergence of **startups with disruptive AI solutions** that are being tested and tested by the Armed Forces of many countries is acting as an accelerating factor of the AI-based dual innovation process.

7. The **EU effort in generative AI is growing,** but it does not seem to be enough to ensure a leading role at the global level in the coming years if investments and the availability of human resources are not strongly accelerated**.**

   The EU has significant weaknesses in the AI value chain, combined with others in the semiconductor sector. In addition, its global investment effort is less extensive and fragmented compared to the strategies of its main competitors (China and the United States).

8. **The EU does not have large digital companies in the generation of AI-based products and services** that allow it to impose its criteria, products, and services on users around the world against its much larger competitors strongly supported by their respective governments.

   The current **European weakness in advanced semiconductor manufacturing** extends to **AI-specific integrated circuits** (such as GPUs, FPGAs, and ASICs), the availability **of cloud software platforms**, and the availability of **large language models (LLMs)** with significant global market quota to serve as the basis for the development of end-user applications.

9. **European AI start-ups have funding problems for their growth in Europe** and run the risk that in their scaling process to be able to compete in global markets they will be acquired or controlled by non-European entities

   The most common risk for European startups in the field of AI is that they will be **acquired by other large non-European companies or migrate to continue their scaling process in the United States**. In addition, they depend on the investment return strategies of specialised investment funds, many of them non-European, that have entered their capital. This situation is especially worrying for those who develop AI-based products or services for defence.

10. The value of **AI-focused innovation ecosystems in the EU** is growing with the participation of large companies and EU and national public administrations as drivers that assume the need to increase **stable interaction between actors** through appropriate programmes and financial instruments.

    This process is less evident due security connotations and a **less open-mindedness of companies and public administrations**, although nuclei of targeted innovative ecosystems are beginning to emerge supported by military procurement and R&D dual-use programmes in various parts of the EU, although with a national perspective.

11. Although the **United States continues to be the country that owns the most well-resourced defence investment funds**, new funds are growing and specialising in defence and security in various European countries, both in the start-up phase and in the scaling phase of new technology companies.

    This situation has also begun to be observed in Spain with a strong involvement of **public financing agencies together with private capital in the initial rounds of financing**. This situation is supported by large investment funds, whether new or with the implementation of specific dual financing vehicles in other preexisting funds.

12. The Spanish defence industry is incorporating AI both in the product generation process using **data-centric digital engineering techniques and simulation** (e.g., digital twins) using AI as an essential factor for increasing the functionality and flexibility of its products.

    The **accelerated use of integrated data management techniques** and the more incipient use of **digital twins** and **3D additive manufacturing** to reduce development cycles and facilitate subsequent operation and maintenance cycles have spread among all large defence programme contractors.

13. The **size limitations of the Spanish defence industry** may prevent it from playing a greater leadership role in the major defence programmes that will be launched in the EU in relation to the strategy to strengthen the industry towards 2030 (*Readiness 2030*) and the commitments of the member states to allocate **additional investment for defence acquisitions.**

    The decisions taken by the EU and the member states to increase resources for the development and acquisition of defence systems to fill **identified gaps** represent an opportunity in the coming years to strengthen the European defence industry and its competitiveness in global markets supported by the incorporation of AI technologies.

14. From the EU's perspective, there is an **opportunity to strengthen the development of AI as a dual technology** by prioritising this issue in public calls and tenders by public administrations whose regulations must be adapted to accelerate the innovation cycle.

    The process of drawing up the EU's 10th Framework Programme for Research and Innovation, the successor programme to the current European Defence Fund, the priorities of the European Defence Agency and the European Space Agency are large opportunities to improve European technological sovereignty in AI if resources and synergies between them are significantly increased.

15. The role of **industry standards and norms for AI products**, as well as **AI-based system certification processes**, is key to achieving a rapid expansion of the market for interoperable intelligent defence systems internationally.

    We are still in an unconsolidated phase in which there are not many specific standards related to military AI or from international organisations. In 2024, in the revised *NATO AI Strategy*, it was decided to establish an *Alliance-wide AI Testing, Evaluation, Verification & Validation (TEV&V)* landscape to ensure the responsible adoption of AI.

Conclusions on the tactical, operational, and strategic dimension of the use of AI by the Armed Forces

1. A **gradual evolution towards an intelligent battlefield** is taking place within the framework of a continuous process of digitalisation that will continue to be very rapid and intense throughout this decade.

   This evolution is being slower in its deployment in the defence sector than in the areas of civilian use given the **relative immaturity of the technologies involved to delegate critical functions to them**, and the need to ensure co-existence with many other pre-existing military systems.

2. The **search for superiority in combat forces** to experiment with technologically immature solutions and accelerate technological innovation, requires close interaction between the Armed Forces, companies and research centres, and universities that allow their integration into future combat strategies and tactics.

   This process has accelerated in recent years through the use of AI solutions in multiple areas supported by the **capture and analysis of near-real-time data** from multiple sensors and the use of synthetic data when appropriate.

3. The **use of autonomous or semi-autonomous AI systems within lethal weapons chains** is technologically feasible, either in the case where their use is limited to the process of identifying and selecting targets or in their direct or indirect neutralisation.

   This use seems to accelerate during the current decade with the emergence or continuation of high-intensity military conflicts in which the use of AI in autonomous or semi-autonomous systems has become a key factor in ensuring superiority in combat.

4. The **need for quality data tailored to the application domain**, whether real or synthetically generated, and protected against cyberattacks, is a prerequisite for the adoption of AI across all socio-economic sectors. In the case of defence, problems persist in having volumes of data obtained under real conditions, which makes the use of generated data even more necessary.

   This need is driven by public administrations or groups of companies creating the so-called **"shared data spaces**". However, in the defence sector many of the datasets relevant to the training of ML systems or LLM are classified and not shared outside military organizations. For this reason, synthetic data have become widespread. Data poisoning and vulnerabilities in the cyberspace domain add to its complexity.

5. **The role of the human being in the decision loop became a key factor from the technical and tactical point of view of AI systems in defence**, regardless of the ethical considerations and the rules of engagement that its use may imply or motivate.

   Acceleration of the technological development of lethal autonomous weapons systems (LAWS) would allow their accelerated incorporation into the armies of all EU Member States, which, if it happens, will imply profound modifications in the way military operations are conducted and in their impact on the population.

6. In the domain of **electronic warfare**, AI plays a growing role. This control has become a key factor in twenty-first century conflicts motivated by the expansion of threats, conflicts, and hybrid warfare superimposed on conventional military conflicts.

   The **increasing complexity of potential attacks on information transmitted by radio space** in military matters (navigation signals, command and control information, satellite data, etc.) makes it necessary to develop new and more sophisticated intelligent electronic warfare techniques capable of detecting signals in the entire frequency spectrum.

7. The **automatic generation of campaigns to disseminate disinformation and narratives** aimed at specific entities or sectors of the population based on AI tools has spread and is in the hands of state or nonstate actors.

This situation comes from a less secure world in which the mastery of information and narrative is essential to determine the course of military operations. The use of generative AI tools for their generation and dissemination on social networks is growing.

8. The EU and its member states have **AI-powered tools and procedures to detect and counter fake news and intentional narratives** from other countries.

   The use of AI tools and procedures is linked to the **need for governments to counteract the growth of interference and manipulation from other countries**, which has forced the creation of specialised units and procedures for the exchange of information between allied governments and rapid alert and response protocols.

9. **The space sector is configured as a dual sector** in which both public and private users can share satellite platforms, launch and tracking systems, data obtained, as well as specific AI tools.

   Individual satellite platforms or constellations are used in civilian and military observation, communications, and navigation applications. Although their structure may be dual, it may require the development of **specialised payloads for each of the domains**. The use for military applications, as *Starlink* in Ukraine showed, has made them essential assets for all governments and, with this, they have acquired strategic relevance for all countries.

10. **AI has increasing value in effectively managing a more populated space domain**, in terms of space objects and fragments, especially in low orbits, which can be used as a military target against assets of other countries.

    AI tools for better situational awareness of the space domain make it possible to reduce or manage the **risks of collision** with satellite debris or other natural elements, **interference** caused or not caused in satellite navigation, and **protection of space assets.**

11. The **development and adoption of AI hardware systems specialised in the operation of space assets** with the aim of reducing consumption and increasing flexibility has increased strongly. This evolution makes it possible to have **greater processing capacity on board** and then, the autonomous execution of more complex functions.

    Space is a dual domain of increasing relevance in which the automation of operations implies the need to increase the processing capacity on board for the execution of AI algorithms, the analysis and filtering of data collected, and its transfer to ground stations.

12. **The EU and Spain are in a good position to exploit the space sector** by developing AI-based applications that exploit the data generated by space assets and thus improve European technological sovereignty in the new generation of space platforms.

The experience accumulated by the *European Space Agency* and various national space agencies in the Member States, together with a profusion of new companies in the space sector with the integration of AI solutions, will make it possible to improve European security if they are provided with sufficient resources. Spain is a relevant player in the space domain.

Conclusions on the ethical and regulatory dimension of AI

1. **There is no specific regulation for the use of AI in defence**. There are only **voluntary guidelines** for use based on the responsible use of AI in the military field proposed by various bodies, but without global acceptance for all countries.

   AI regulations for civilian applications are also not agreed upon and many countries have different approaches based on their historical-cultural visions and their technological positioning in global markets. However, the EU AI Regulation could be used for the development of dual AI systems.

2. The increasing **availability of automated intelligent systems without requiring a human being to make the necessary decisions** that the development of AI already allows implies assuming considerable ethical risks, especially in the case of the use of lethal autonomous or semi-autonomous weapons systems (LAWS).

   The EU should be aware that the regulations for the use of LAWS must be agreed as far as possible at a global level, establishing limitations on their development and use. If this is not the case, as is currently the case, there is a risk of asymmetrical confrontations in its use that can reach not only state-based armies but also other armed groups whose rules of use are unpredictable or not subject to rules.

3. The **development of products based on dual technologies by companies outside the defence sector** has generated problems arising from the acceptance of projects of potential military utility by their technical staff, as it was considered that there was no explicit prior acceptance and that their ethical principles were contravened.

   This situation may grow in the future as budget increases and the continued civilian push for the development of AI technology means that more companies outside the defence world until now will be involved in the development of intelligent defence systems.

4. The ethical problems of AI-based military decision support systems cannot be analysed as isolated systems, but by **the role they assume in the integration into lethal chains, whether automated or not.**

This problem has already arisen with the use of AI-based tools by Israel in Gaza which, although not a lethal weapon in itself, can attack targets previously identified by the tool with a percentage of wrong targets.

5. Although there have been many **efforts by international organisations to achieve responsible use of AI**, even in dual or strictly military applications, their results are, for the moment, limited to reaching a detailed and effective global agreement.

   These agreements are not expected to go beyond the approval of a set of voluntary implementation guidelines that the signatory countries accept, but without the existence of international organisations to ensure their compliance with them, as is the case with nuclear weapons.

6. Finding the **balance between a regulation that protects the user and supports innovation** is not easy, and that debate is still open in the context of the European Union in the process of implementing its AI regulation designed only for civilian and not military applications.

   The EU will need to adopt a flexible approach during the implementation of the regulation, ensuring consistent interpretations across Member States, and regularly adapting AI regulation to technological developments to ensure its relevance.

7. The **progressive integration of AI with neurotechnology** opens the way to a new phase of military conflicts with specific ethical problems such as those of privacy and agency in the context of the discussion of neurorights and their application in defence.

   The field of neurotechnology applied to improving human cognitive abilities, beyond medical use, has enormous **ethical implications in terms of altering the capacities of the human species**. Its development in the field of defence is carried out with little transparency on the part of the most advanced powers aware of its potential future relevance.

8. A factor that will condition the development and use of AI in military operations is the possible **military confrontation between adversaries with different ethical and moral frameworks in the use of autonomous systems.**

   This factor may condition self-limitation in the use of certain smart weapons so as not to be at a disadvantage against the adversary, which means that the use of AI in these contexts should be limited, at least, to reaching “no first use” commitments, as is already the case in certain countries with the use of nuclear weapons.

9. **Technologies for increasing cognitive abilities,** beyond what the human species allows in its biology, through the **convergence between neurotechnology and AI,** is still a distant

issue in terms of mass adoption, but which, in view of its accelerated development, will imply anticipating ethical measures.

The technological feasibility of the convergence of neurotechnology with AI is closer in time. The use of synthetic biology techniques on neuronal tissue and its convergence with neurotechnology and artificial intelligence is also advancing rapidly. This process of multi-technology convergence forces us to think about the ethical and regulatory consequences derived from becoming a reality with years to come.

Conclusions on European Technological Sovereignty in AI

1. Given the strategic relevance of technology, the EU's objective of achieving its long-awaited **strategic autonomy involves increasing its technological sovereignty**.

   This objective must be pursued, even accepting the impossibility of achieving autarky in AI, for which it will be necessary to have reliable long-term allies.

2. EU States members rely on **multiple defence systems that incorporate AI functionalities** developed locally or from other countries with only **partial knowledge transfer for external providers.**

   Military equipment for EU countries from the United States and, to a lesser extent, from the United Kingdom, Israel, Turkey, South Korea, and Japan is relevant. For advanced weapons systems, their acquisition implies the **acceptance of restrictive conditions of use** and is subject to use permits in various cases imposed by the respective suppliers in concert with the governments of the parent companies.

3. The future development of military AI systems with a **high degree of European technological sovereignty** will require establishing and financing significatively common public-private programmes supported by sustained political will with long-term priorities.

   This will be a long and complex process since the main competences in defence policy lie with the member States, beyond the coordination and use of resources related to industrial policy that can be made from the EU budget.

4. It will not be possible to achieve a sufficient level of technological sovereignty if the **fragmentation of the European defence market** is perpetuated in weapons systems that incorporate, in a relevant way, artificial intelligence modules.

   The speed at which AI-related technology is developing makes it difficult for the industry of a single member state to possess all the necessary capabilities for the autonomous

development of intelligent military systems. For this reason, **stable technological cooperation between players in the defence industry in a single market** should be a priority policy objective.

5. A significant part of the **continued increase in investment in defence technology systems** in relation to GDP agreed by EU NATO member States should be allocated to **investments in interoperable intelligent systems**.

   The discussion to implement the agreement to increase defence spending in relation to GDP agreed at the NATO Summit in June 2025 should prioritise the development of interoperable AI systems within the framework of NATO with a greater European effort to reduce the EU's dependence on the United States.

6. **Startups with disruptive AI products find it difficult to experiment with solutions in low states of maturity (TRL 5-6)** together with the armies that accelerate the innovation process and adapt to the requirements of the Armed Forces of the EU Member States.

   The solution should involve the creation of focused instruments for public procurement of technology by the Government, and necessary regulatory modifications by the EU and the Member States. The measures proposed by the EIF to **promote deep-tech entrepreneurship** constitute useful contributions in this perspective.

7. The **administrative simplification strategy** promoted by the EU will have to be promptly adapted to the defence sector to drastically reduce the times of contracts for the acquisition and maintenance of new weapons systems involving the use of EU funds.

   Although this situation is not exclusive to AI and affects other emerging technologies, it is clearly manifested in the development and acquisition of autonomous systems in which progress is very rapid, as shown by the experience from Ukraine.

From the conclusions drawn from the analysis performed in this report, **the EU is at a critical moment** where it must act decisively to take control of its own development of AI and ensure its rapid uptake by its armed forces. Other major technological powers with which it competes have assumed this reality and **prioritised the development and use of AI**, aware of the essential role they play in the search for military supremacy.

Possible scenarios of European technological sovereignty in AI

Based on the conclusions made, three **possible scenarios for the EU in AI in defence** in the horizon of 2030 have been identified and assessed, which are detailed below. We are aware that these are **basic scenarios to promote open discussion** and to be able to analyse

in detail, if desired, the situation in the EU as a whole or in some of the Member States. The three scenarios identified have been called the **"optimistic"** scenario, the **"realistic"** scenario, and the **"pessimistic"** scenario.

Optimistic scenario by 2030

The optimistic scenario assumes that the **EU becomes a global AI technological power**, leading alongside the United States and China in the development and use of AI in defence.

This scenario is characterized by the following **defining features**.

- Creation of a European **single market for defence** that significantly reduces current fragmentation and maximises the outcome. This will make it necessary to make the necessary regulatory modifications in the framework of EU Treaties to give more responsibility to the European Commission in the implementation of the EU industrial defence policy.
- Achieving **high technological sovereignty in AI applied to defence**, from the ability to design and manufacture specific AI hardware to the development of applications integrated into military systems.
- Launch of large **R&D community programmes in defence**, emphasising the application of AI fully integrated with national programmes.
- Emergence of **large European AI companies in defence** that have become world leaders in some of the areas of application.

Realistic scenario by 2030

The realistic scenario assumes that the **EU becomes a relevant technological power in the development and use of AI in defence with leadership in some specific technical areas** but dependent on other powers in the rest of the relevant technological areas in AI.

This scenario is characterised by the following defining features.

- The creation of a European single market for defence has not met all its objectives, but there has been a **greater synergy of actions** with the significant reduction of the current fragmentation in some defence priority areas.
- Some **regulatory modifications** have been made to facilitate the adoption of joint agreements in the field of defence using enhanced cooperation schemes coordinated with NATO.
- Achieving **limited technological sovereignty in AI** applied to defence with improved AI-specific chip design capabilities and the development of integrated applications in military systems, although dependence on external component and manufacturing suppliers persists.

- Implementation of **community R&D programmes in defence with limited resources** that emphasise the application of AI and are coordinated with the national programmes of countries that wish to do so.
- **Strengthened strategic cooperation of large national AI companies in defence** to ensure global leadership in some AI application areas.

Pessimistic scenario in 2030

The pessimistic scenario assumes that the **EU does not become a global technological power in the development and use of artificial intelligence in defence**, consolidating its dependence on other countries.

This pessimistic scenario, which means a continuity of the current situation, is characterised by the following features:

- The EU has **limited technological sovereignty in AI for defence**, so its dependence on the United States in large military systems persists.
- **Defence R&D programmes are basically national** with objectives of national technological independence, although there are some projects co-financed with the EU budget and contributions from Member States on a voluntary basis.
- **No large European companies with high AI capabilities in defence have emerged**, and strategic cooperation between relevant companies remains very limited.

The realistic scenario could be achieved by 2030 if the necessary resources were allocated and there was a long-term adequate political will. The conviction of the Member States that the conflictive global situation will force the EU to coordinate its defence actions much better and make agreements more feasible to achieve this scenario will contribute to this. The following section aims to offer, based on the conclusions drawn, a set of **recommendations for action** so that the realistic scenario presented can become a reality in 2030.

Recommendations for Action

From the conclusions made, a **reduced set of recommendations for action** is proposed for the regulation, development, and advanced use of AI in defence systems to increase its responsible use in the European context and achieve the realistic scenario outlined in the previous section. The **proposed recommendations for action are not entirely disjoint**; in fact, achieving a high impact on the operation of the Armed Forces of the EU member states through them may make it advisable to **implement several of them simultaneously and in coordination.** The proposed action recommendations are as follows:

Recommendation R1. Prioritisation of AI in Member States' R&D defence and military procurement programmes with a dual-use vision.

The EU and Member States should **step up efforts on the dual use of AI by setting specific priorities** in their public research and procurement programmes and facilitating the use of its results in both civilian and military markets.

This recommendation should be part of the **negotiation process of the EU's Framework Programme for Research and Innovation HE 2028-2034** and the future **European Defence Fund** funded under the *EU's Multiannual Financial Perspectives* (2028-2034).

Recommendation R2. Need to create a common regulatory framework for the development and use of AI in defence in line with European principles and values.

It is necessary to establish as quickly as possible a **common regulatory framework for the use of AI in defence** based or not based on the existing AI Regulation. Although regulations are legally limited to Member States, their use can be voluntarily extended to other allied countries.

The **adaptation of the current EU AI Regulation to cover its dual uses** is not clearly defined. This is a process that could be carried out in parallel and independently of the promotion of a specific regulation for military AI using, if necessary, a model of enhanced cooperation between those Member States that consider it appropriate or, failing that, a homogeneous and coordinated set of guidelines of voluntary application.

Recommendation R3. Facilitate accelerated experimentation of the use of AI in the Armed Forces of EU Member States to accelerate its adoption.

It is necessary to facilitate the **experimentation of the advanced use of AI** in the Armed Forces of EU Member States to assess the effectiveness and risks that its use may entail in applications linked to decision-making.

The experience gained in Ukraine allows for a drastic reduction in development times if experimentation in real conditions is incorporated into the life cycle. Their implementation may involve the **provision of shared physical and defence data spaces** in the Member States but accessible to others under pre-established conditions. It would be possible to leverage the network of test centres of the DIANA programme deployed in NATO's member states that have an AI relationship.

Recommendation R4. Extend the scope of the European Semiconductor Regulation (Chip Act) to address the development of AI chips for defence.

The aim is that, in the shortest possible time, the EU will have a value chain of semiconductors for defence that allows it to have the specific chips it requires for the development of its weapons systems with the minimum of external dependencies.

The **extension of the Chip Act** with additional resources to include various actions aimed at having specific AI integrated circuits for defence systems with the highest possible degree of European technological sovereignty. Spain could promote a pilot line of AI chips for defence.

Recommendation R5. Increase efforts in attracting, retaining and training AI specialists in areas of interest to defence.

Given the rapid evolution of AI-related technology and its convergence with other emerging technologies, the **EU will need to increase efforts to attract, retain, and train AI specialists** who can be employed by the defence industry and the Armed Forces to accelerate their uptake in Europe.

The **EU should reduce the shortage of AI specialists** by creating joint training programmes between several countries supported by the European Commission and the defence industry to update knowledge. Training priorities should be aligned with the EU gaps identified in the *Defence White Paper*. From an instrumental point of view, one possible option is to take advantage of *European university networks* and the creation of a **specific transversal programme** with actions in the HE 2028-2034 co-funded with EU and EU Member State resources.

Recommendation R6. The EU should support the creation and strengthening of national AI ecosystems in defence.

Support for the creation and strengthening of **national AI ecosystems in defence** is understood as a prerequisite for the **creation of a flexible and sufficiently integrated "European ecosystem"** to improve European positioning in a highly competitive global context.

National ecosystems should focus on the areas of AI applied to defence in which there is a strong industrial fabric and favour the development of large projects of common European interest in which AI is a key technology. One option is to build on the effort already made by the European Commission with the so-called *AI factories*, to evolve some of them with a dual approach, and ensure their relationship and interaction with the Armed Forces and the defence industry.

Recommendation R7. Launch a European defence accelerator based on cooperation between the European Commission and Member States.

To launch the creation of a European accelerator with a specific line of support for disruptive AI startups of a dual nature based on public-private participation and cooperation and the participation of Member States that wish to do so through national defence accelerators.

The aim is **to avoid or limit a fragmentation of the acceleration process**. One option for implementing the accelerator is its integration into the **European Innovation Council (EIC),** although with the specificities of the defence sector, as well as its alignment with the EIT by redefining its performance in low TRLs, and the accelerators of **NATO's DIANA** programme, one of them located in Spain.

Recommendation R8. Update Spain's Defence Technology Strategy 2020 (ETID 2020) until 2030 by prioritising AI technologies aligned with the EU's *Readiness 2030* programme.

Update the Ministry of Defence's ETID 2020 to align it with the European Commission's "*Readiness 2030*" priorities, the *European Defence Programme*, *NATO's priorities in relation to AI,* and related Spanish defence and security programmes.

The update should be carried out as soon as possible in order to better compete with other countries and to have a national support framework that increases Spanish participation and leadership in the future EU Framework Programme for Research and Innovation "*Horizon Europe 2028-2034*".

Recommendation R9. Aligning European strategy with realistic scenarios for achieving technological sovereignty in AI for defence.

The detailed analysis of European and Spanish technological sovereignty in AI for military use must be aligned with the **feasible scenarios toward 2030** that are to be jointly promoted from a realistic position of the European situation.

The WG members consider that the **realistic scenario** indicated above is appropriate for Spain and should be reached. In any case, it is considered necessary to **periodically reassess the situation of European technological sovereignty in AI using synthetic indicators** for this purpose and to define a new realistic scenario achievable in the period 2030-2035 that takes into account the evolution of AI technology and the milestones achieved by the EU in the development and sovereign use of AI in defence until 2030. This alignment must contemplate updating the priorities established for defence in areas related to AI.

Recommendation R10. Establish a Defence AI Observatory with a multidimensional perspective at the service of all Member States and coordinating national efforts.

It is considered necessary to create an **AI in Defence Observatory** to assess the evolution from the scientific-technological, socio-economic, tactical and operational in the armies, and ethics and regulatory dimensions. It is not, therefore, a question of technology watch, but also of markets, users and the context in which it is used.

This *Observatory* could be **coordinated by the European Commission**, with the European defence industry and with the participation of external experts. The *Observatory* should also coordinate its activities with NATO and, on specific issues, with those existing in other allied countries with the necessary levels of confidentiality. Part of the documentation generated could be considered as **classified**.

Final remark

This report has presented a **very dynamic scenario of the use of AI in defence** driven by supremacy goals of large powers and constrained by geopolitical risks. Current intensive military conflicts are acting as boosters of the development and deployment of AI-based systems in the battlefield which accelerates decision making. Then, technology, economy, military, an ethical and regulatory perspectives are deeply intertwined,

Within this context, **the EU faces an urgent and deep challenge to be able to play a role in this AI global race**. To address it, the EU should reduce fragmentation, provide abundant resources, both human and material, conduct smart regulatory changes, and sustained political will. All of them should be compiled and integrated to successfully concur in the global scene.

COMPOSITION OF THE WORKING GROUP

The **working group** was composed by the following members[02]:

- **Gonzalo León** (Coordinator) (FEI and Emeritus professor UPM)
- **Luis Fernando Álvarez-Gascón** (FEI and Secure eSolutions GMV)
- **Txema Báez Cristóbal** (FEI and NOVADAYS)
- **Juan Carlos Dueñas** (Professor UPM)
- **Ángel Gómez de Agreda** (Col (R) of Air&Space Army and Europavia Middle East)
- **Asunción Gómez-Pérez** (Professor UPM)
- **Luis Guerra** (FEI and Oesia Group)
- **José María Insenser Farré** (FEI, AMETIC IPCEI)
- **Juan Bosco Morales de los Ríos** (CTO AMPER Group)
- **David Ramírez Morán** (IEEE-CESEDEN Analyst)
- **Luis Vázquez Martínez** (FEI and Emeritus professor UCM)

Technical support and collaboration of:

- **Aureliano da Ponte** (UCM researcher and defence consulting)
- **José Sousa** (AMPER Portugal)

During the meetings of the Working Group, the following persons have been invited to enhance the perspectives of the analysis:

- **Manuel Pérez Cortés** (Director Defence Area of GMV)
- **Ricardo Sáenz** (Director of Defence and Security Programmes of GMV)
- **GD Guillermo Ramírez Altozano** (Director of Information Systems, Telecommunications and Technical assistance (JCISAT) of the Spanish Land Army
- **GB Roberto Villanueva** (Former director of Cybersecurity of CESTIC, Ministry of Defence)
- **Claudio Feijóo** (Professor of UPM. Chair Jean Monnet of Technology Diplomacy and Digital Sovereignty).
- **GD (R) Juan Antonio Moliner** (Vice-president of the Academy of Military Sciences and Arts, ACAMI)
- **Carmen Vela** (President FEI) and **Pedro Morenés** (President Amper Group) have also participated in some meetings of the working group.

02 More extensive CVs of WG members and invited experts can be found in the full version of the report.

Abridged version of the final report

Situation and trends in the use of artificial intelligence in the defence sector

september 2025


ABB


aertec
SOLUTIONS


AIRBUS


AIRBUS
DEFENCE & SPACE


AMADIX


ANTOLIN


ayming


CCOO


Fundación
Caja Rural
de Asturias


Fundación
General CSIC


FUNDACIÓN
Parque Científico
de Madrid


gmv
INNOVATING SOLUTIONS


ienai [SPACE]


innovairv


MERCK


MSD
INVENTING FOR LIFE


Poile
ingenieros s.l.


sacyr


SAVANA
The AI + RWE Company


Smart
Agrifood


tecnalia


Talgo


uc3m
Parque
Científico