Instituto Español de Estudios Estratégicos

Research Paper

[Visitar la WEB](#)

[Recibir BOLETÍN ELECTRÓNICO](#)

01/2026 13/01/2026

Sonia Benito Hernández, Antonio Fonfría Mesa and David Ramírez Morán

Defence 5.0: Strategic Challenges and Technological Opportunities for Spain

Defence 5.0: Strategic Challenges and Technological Opportunities for Spain

Abstract:

In the current context of technological and geopolitical transformation, Spain faces a structural challenge: the low growth of the total factor productivity, particularly in its industrial sector, compared to other European Union countries. This weakness limits its competitiveness and innovation capacity, making an urgency of the adoption of advanced technologies and its effective integration in the business model. In the field of defence, this challenge acquires a strategic dimension, as mere participation in international consortia is not sufficient; it is a necessity to consolidate a national innovation ecosystem, capable of generating sovereign, sustainable technologies aligned with the country's priorities and needs. Achieving this requires the development of critical capabilities such as cybersecurity, artificial intelligence applied to military environments, or smart naval industry, as well as fostering public-private collaboration and strengthening technology transfer between universities, research centres, and companies. This approach would help reduce external technological dependence, reinforce European strategic autonomy, and position Spain as a relevant actor in the global landscape. Within this framework, the central research question guiding this study is: Can Spain consolidate a national defence innovation ecosystem that enhances its productivity and technological autonomy?

Keywords: industry 5.0; technological development; strategic defence; collaborative ecosystem; national autonomy.

How to cite this document:

BENITO HERNÁNDEZ, Sonia; FONFRÍA MESA, Antonio; y RAMÍREZ MORÁN, David. *Defence 5.0: Strategic Challenges and Technological Opportunities for Spain*. Research paper IEEE 01/2026. IEEE web link and/or enlace bie[3] link (consulted day/month/year)

1. Introduction

The 21st century is characterized by an unprecedented acceleration of technological evolution, with a direct impact on all areas of human life, including security and defence. After the consolidation of the Industry 4.0 paradigm—focused on digitalization, automation, and intensive data use—Industry 5.0 is beginning to emerge, a concept that seeks to go beyond productive efficiency to place human beings, sustainability, and resilience at the centre of production processes.

Industry 4.0, also known as the Fourth Industrial Revolution, was popularized by Schwab (2016), founder and executive chairman of the World Economic Forum, who defined it as a revolution unique in its scale, scope, and complexity due to the fusion of physical, digital, and biological spheres and its cross-cutting impact on institutions, industries, and individuals. Schwab placed the beginning of this paradigm shift at the end of the 20th century and the start of the 21st, driven by mobile Internet, more powerful and affordable sensors, and the evolution of artificial intelligence and machine learning. Thus, the Fourth Industrial Revolution does not arise from an isolated innovation but from the accelerated convergence of multiple technological developments that redefined production models, employment, and social interaction. In the field of defence, these technologies enable process automation, improved operational decision-making, and the development of autonomous and connected systems. According to Corzo-Ussa et al. (2022), the application of Industry 4.0 in defence represents a strategic opportunity to reduce technological gaps and strengthen sovereign capabilities in countries such as Spain.

Industry 5.0, promoted by the European Union since 2021 (Carayannis & Morawska-Jancelewicz, 2022), represents an evolution of the previous paradigm. This approach incorporates ethical and social principles into the design of technological systems, prioritizing collaboration between humans and machines and sustainability in both environmental and social dimensions. Travez Tipan and Villafuerte Garzón (2023) emphasize that this new stage relies on technologies such as AI, IoT, extended reality, and cobots (collaborative robotics), but with a focus on social value and technological responsibility. Thus, while Industry 4.0 is characterized by intensive automation, digital interconnection, and the use of technologies to optimize production processes, Industry 5.0 proposes reintegrating the human being at the centre of the production system through collaboration with an evolution of these technologies, steering innovation towardss sustainability, resilience, and social well-being (Pérez-Domínguez et al., 2023).

Recent literature, along with leading authors in fields such as industry, marketing, engineering, and business, highlights this transition. Among the key works is Marketing 5.0: Technology for Humanity by Kotler et al. (2021), which analyzes how emerging technologies not only transform production but also the relationship between institutions, companies, and citizens. From a strictly industrial perspective, notable publications include Industry 5.0: Concepts and Strategies for Digital Transformation (Kaswan et al., 2023), which addresses the role of artificial intelligence (AI) and digitalization in this new era. Likewise, works such as Smart Organizations in Industry 5.0: A Human-Centric Approach (Saniuk et al., 2022) and Industria 5.0: a human-centredcentred approach (Castellanos Alba, 2023) reinforce the idea that the new paradigm is not limited to technical aspects but incorporates ethical, social, and sustainability considerations.

In parallel, various international forums serve as reference spaces for debate and consensus-building around Industry 5.0. Among them are the World Industry 5.0 Forum, which addresses the convergence of technology, sustainability, and human innovation; the Transfiere Forum, held in Málaga, which has become a European meeting point for science and technology; and events such as the People and Industry Forum in the Era of Society 5.0 (University of the Andes, 2025) or the Forging Forum, which highlight the interaction between industrial development, environmental responsibility, and social well-being. Also noteworthy is the International Workshop on Industry 5.0 and Society 5.0 (IWIS), which brings together international researchers to analyze both the benefits and barriers of this new paradigm.

In the case of Spain, the transition towardss 5.0 economy requires smart reindustrialization, based on digitalization, sustainability, and resilience. According to the report prepared by PwC and Siemens (2025), this transformation could increase the share of industry from 16% to 18% of GDP over the next decade, provided that strategic investments in infrastructure, talent, and disruptive technologies are prioritized. At the same time, Spain is fully integrated into a shared security ecosystem, both within the framework of the European Union and NATO. In this context, technological innovation becomes a key factor for strengthening interoperability with allies and ensuring strategic autonomy. European programs such as the European Defence Fund (EDF) and the

Future Combat Air System (FCAS) project, along with national initiatives promoted by the Ministry of Defence, reflect a growing commitment to the disruptive innovation represented by this revolution.

Moreover, the serious problem of the lack of growth in total factor productivity in the Spanish economy—and particularly in its industry—compared to other EU countries, is a key factor for adopting new technologies. In this context, the challenge for Spain goes beyond mere participation in international consortia and requires the consolidation of a national defence innovation ecosystem capable of generating sovereign and sustainable technologies over time. This involves not only boosting critical capabilities in areas such as cybersecurity, artificial intelligence applied to the military environment, or smart naval industry, among others, but also promoting public-private collaboration, strengthening technology transfer between universities, research centres, and companies, and ensuring that the solutions developed respond to the country's strategic priorities. Ultimately, building this ecosystem is essential to reduce external dependencies, reinforce European strategic autonomy, and position Spain as a relevant player in the global technological landscape of defence.

For this reason, analysing the transition from Industry 4.0 to Industry 5.0 in the defence sector is crucial to identify both the strategic opportunities and the risks arising from this process. Spain, as a middle power with a relevant role in European and Mediterranean security, cannot adopt a merely receptive position towards foreign technologies. Innovation in defence not only contributes to improving military effectiveness but also generates positive effects on the national economy, fosters highly skilled employment, boosts international competitiveness, and provides the Armed Forces with the appropriate means to face the current conflict, in which technology, as has historically been the case, constitutes a key element for measuring the operational capacity of armies.

On the other hand, the transition towards Defence 5.0 poses cross-cutting challenges that go far beyond purely technological aspects, integrating ethical, legal, and strategic dimensions. Among these is the need to establish clear frameworks for the responsible use of artificial intelligence, ensure the regulation and oversight of autonomous systems in military operations, and promote sustainability practices throughout the production and maintenance chain of the defence industry. Additionally, strengthening resilience against cyber threats is essential, given that the interconnection of systems and dependence on advanced digital platforms increase both exposure to risks and the criticality of infrastructures. This set of challenges underscores that Industry 5.0 is not merely a matter of technological innovation but a complex process of institutional and strategic transformation.

The central purpose of this paper is to analyse the transition from Industry 4.0 to the so-called Industry 5.0 in the defence sector, paying special attention to the challenges and opportunities that this transformation poses for Spain. In this regard, the article aims, first, to clearly define the concept of Defence 5.0 and highlight its differences from the previous paradigm. It also seeks to examine Spain's role in this process of change, both in its integration within the international framework—through the European Union and NATO—and in strengthening a national innovation ecosystem capable of generating its own capabilities.

The article also intends to explore in detail the application of 5.0 technologies in different defence subsectors, from the aeronautical, land, and naval domains to consulting and engineering, cybersecurity, and the emerging ecosystem of startups and deep-tech companies. The goal is to provide a comprehensive view of how innovation materializes in different areas of the Armed Forces and the national industry, and how it can contribute to strengthening Spain's strategic autonomy and technological competitiveness. Finally, it seeks to identify the main challenges posed by Defence 5.0—such as technological sovereignty, interoperability with allies, or ethical dilemmas arising from the use of autonomous systems—and, at the same time, point out the opportunities it offers in terms of European leadership, industrial development, and the strengthening of national security.

In this context, it is pertinent to ask how Spain can leverage this transition to strengthen its strategic autonomy and technological development in defence. Therefore, the research question guiding this study can be formulated as follows: How can Spain take advantage of the transition towards Defence 5.0 to reinforce its strategic autonomy, its capacity for innovation, and its role within the European, Atlantic and global security frameworks?

The structure of the article follows this logic of progressive analysis. Section 2 focuses on explaining the evolution from Industry 4.0 to 5.0, with an emphasis on the specific implications of this change for the military domain. Section 3 presents an overview of Spain's situation regarding defence innovation, paying attention to both institutional frameworks and key industrial actors. Section 4 addresses the sectoral application of 5.0 technologies in different areas of defence. Finally, Section 5 offers the conclusions of the paper, synthesizing the main findings and outlining future perspectives within the horizon of Defence 5.0.

2. From Industry 4.0 to 5.0 in the Defence Sector

2.1 Key Technologies of Industry 4.0: Limitations and Challenges in the Military Domain

In the field of defence, Industry 4.0 has enabled the transformation of planning, operation, and maintenance of military systems through intelligent automation, real-time connectivity, and predictive analytics. Among the main technologies applied to defence are:

- Internet of Things (IoT) and its military derivative, the Internet of Battlefield Things (IoBT), which enables the interconnection of sensors, vehicles, weapons, and logistics systems to improve situational awareness and real-time decision-making (Riola et al., 2020).
- Artificial Intelligence (AI), used for operational data analysis, threat detection, logistics optimization, and control of autonomous systems (Corzo-Ussa et al., 2022).
- Big Data and advanced analytics, which allow processing large volumes of information from multiple sources (satellites, radars, tactical networks) to generate operational and logistical intelligence.
- Robotics, applied to tasks such as demining, surveillance, maintenance, and logistical support in hostile environments.
- Digital twins, which virtually replicate military systems to simulate scenarios, predict failures, and optimize performance.
- Virtual Reality (VR), employed in training, tactical simulation, and crew support.

These technologies not only improve operational efficiency but also enable greater adaptability in complex and dynamic environments, such as modern combat scenarios. Their implementation, however, poses challenges in terms of interoperability, cybersecurity, and technological dependency. Although Industry 4.0 has introduced significant advances in the defence sector, its implementation faces structural, strategic, and ethical limitations. Furthermore, interoperability between legacy systems and new digital platforms represents a considerable technical challenge. Armed Forces must integrate disruptive technologies without compromising the stability of existing infrastructures or short-term operability, which requires substantial investments in modernization and cybersecurity. From a social and labor perspective, intensive automation can generate structural unemployment in sectors linked to defence, particularly affecting routine and operational tasks. According to Lodeiro Encina (2018), this transformation may cause social tensions if not accompanied by training and professional retraining policies. Employers must also adapt their practices to value appropriate skills, understand the new risk environment in which they operate, and adjust company procedures and personnel to accommodate new paradigms in both production and related products and services.

Moreover, the use of technologies such as artificial intelligence in weapons systems raises ethical dilemmas regarding autonomy in lethal decision-making, legal responsibility in armed conflicts, and human oversight in critical operations. One of the main risks is delegating critical decisions to autonomous systems, which can lead to situations where there is no clear attribution of responsibility in cases of violations of International Humanitarian Law (Barroso & Pérez, 2025). Additionally, AI can reproduce algorithmic biases that affect target identification, increasing the risk of collateral damage or unjustified attacks. Barroso & Pérez (2025) warn that, without adequate regulatory frameworks, the implementation of AI in defence may violate fundamental rights and create scenarios of technological impunity. From a sustainability perspective, the massive deployment of AI in defence entails high energy consumption (Atausinchi Masias et al., 2025), intensive use of natural resources (such as water and rare minerals), and a significant carbon footprint. The technological infrastructure required to operate autonomous systems, data centres, communication networks, sensors, etc., contributes to the environmental impact of the military industry, demanding a critical review of its compatibility with global sustainability objectives.

Regarding other technologies, the use of sensors, drones, autonomous platforms, and intensive surveillance systems poses risks of privacy violations, combat dehumanization, and delegation of critical decisions to automated systems. For example, the use of computer vision and classification algorithms in intelligence operations can generate biased or erroneous interpretations that affect fundamental rights.

Additionally, technologies such as military blockchain and tactical IoBT require highly secure and energy-intensive infrastructure. This creates a conflict with sustainability principles, as encryption, constant connectivity, and distributed processing increase energy consumption in environments where resources are limited (Atausinchi Masias et al., 2025). Recent research has proposed low-power sensors and efficient cryptographic protocols, but challenges remain in spectral efficiency and technological waste management. In terms of environmental sustainability, the deployment of 4.0 technologies in defence can affect sensitive ecosystems (Calderón Leyton, 2024), especially in training or deployment areas. Finally, technological dependence on foreign suppliers for critical components (sensors, software, processing and infrastructure devices, algorithms…) poses a strategic dilemma: Can a country guarantee its technological sovereignty without compromising ethics and sustainability?

2.2 Concept and Principles of Industry 5.0: From Digital Defence to Cognitive and Human-Centric Defence

Industry 5.0 represents an evolution of the technological paradigm that dominated the Fourth Industrial Revolution. While Industry 4.0 focused, as previously noted, on automation, digitalization, and operational efficiency through technologies such as the Internet of Things (IoT), artificial intelligence (AI), big data, and cyber-physical systems, Industry 5.0 introduces a more holistic approach. This new paradigm does not seek to replace previous technology but to complement it, redirecting its objectives towards creating social value, respecting planetary boundaries, and ensuring workers' well-being. In the words of Carayannis and Morawska-Jancelewicz (2022), Industry 5.0 "places people at the centre of the production process" and redefines the purpose of industrial innovation as a means to achieve social and environmental goals.

Fundamental Principles of Industry 5.0

The European Commission has defined three essential pillars for Industry 5.0: human-centricity, sustainability, and resilience. It emphasizes the importance of considering the human factor as a substantive axis in innovation and sustainable development processes, especially in complex industrial and technological environments. These principles have direct implications for the defence sector (Carayannis & Morawska-Jancelewicz, 2022):

1. Human-Centric: Technology must serve the operator, facilitating their work, protecting their physical and mental health, and respecting their dignity. This includes the design of ergonomic systems, the inclusion of cobots (collaborative robots), and the involvement of personnel in the development of new technological solutions.
2. Sustainability: The industry must reduce its ecological footprint, optimize the use of natural resources, and adopt circular economy practices. Technologies such as additive manufacturing, AI for energy efficiency, and digital twins for predictive maintenance are key in this process. These technologies also help manage and make the most of scarce resources.
3. Resilience: Systems must be robust against disruptions, adaptable to changing contexts, and capable of operating in highly uncertain environments. This involves developing secure critical infrastructures, redundant networks, and rapid response capabilities to cyberattacks or systemic failures.

One of the key concepts in this transition is that of the Resilient Operator 5.0. While the Operator 4.0 was conceived as a technology-assisted agent capable of interacting with automated systems, the Operator 5.0 is an active subject who participates in the design, implementation, and supervision of the technologies they use (Carros Suárez & Sarmiento Paredes, 2022). This new role requires advanced cognitive skills, training in technological ethics, competencies in cybersecurity, and the ability to adapt to complex environments. Cognitive defence is based on this figure, which combines human intuition with technology-enhanced capabilities.

Aligned with this well-being-centred approach, the concept of 'Hospitality 5.0' is adapted to the military environment to ensure safe, hygienic, and well-being-oriented operational settings. This includes the use of environmental sensors, health monitoring systems, and human-machine interaction protocols that minimize stress and fatigue (Carros Suárez & Sarmiento Paredes, 2022).

The transition towards Defence 5.0 relies on a set of enabling technologies that allow the implementation of the principles mentioned above:

- Digital twins: Virtual models of military systems that allow simulation, prediction, and operational optimization. They are key for predictive maintenance, strategic planning, and advanced training.
- Cobots and collaborative robotics: Robots designed to interact safely with humans in complex or strenuous tasks, such as heavy lifting, extended activity sessions, or prolonged surveillance, ranging from logistics to tactical operations.
- Explainable AI: Algorithms that are not only efficient but also transparent, auditable, and aligned with legal and moral principles.
- Augmented reality: Tools for immersive training, decision-making support in the field, and visualization of operational data.
- Bio-inspired technologies: Systems that mimic natural processes to improve energy efficiency, adaptability, and sustainability.
- Cognitive platforms: Systems that integrate natural language processing, pattern recognition, and machine learning to support operational intelligence.

These technologies not only transform how combat is conducted but also how planning, training, and operator protection are approached. In the transition from Industry 4.0 to Industry 5.0 in the defence sector, there is a significant evolution in the technologies employed—not only in functional terms but also in their strategic orientation. The following table presents a comparison between the main technologies used in each paradigm, highlighting how the 5.0 approach introduces elements focused on human-centricity, sustainability, and resilience. This transformation does not imply a complete replacement of previous capabilities but rather a reconfiguration that seeks to integrate cognitive, emotional, and ethical dimensions into the design and application of technological solutions for defence

Table 1. Determining Factors: From Industry 4.0 to Defence 5.0.

Defence 4.0 Technologies	Defence 5.0 Technologies	Key Differences
Internet of Battlefield Things (IoBT) *Smart perimeter surveillance system in military bases.*	Tactical Internet of Things focused on the operator *Tactical combat cloud with cognitive intelligence, adaptive resilience, and human prioritization.*	Industry 4.0: Connects devices and systems for data exchange and remote control. Industry 5.0: Adapts to the human operator and prioritizes safety and well-being in critical environments.

Artificial Intelligence (AI) *Satellite image analysis system for target detection.*	Explainable AI *Autonomous lethal weapons systems (LAWS)*	Industry 4.0: Optimizes processes and automates decision-making. Industry 5.0: Must be transparent, auditable, and aligned with ethical principles, ensuring trust and accountability. Industry 5.0 includes Industry 4.0 and complements it.
Big Data & Analytics *Profiling and disinformation*	Cognitive and contextual analytics *Cognitive warfare*	Industry 4.0: Analyzes large volumes of data to improve efficiency. Industry 5.0: Contextualizes with human perception, integrating social and cognitive factors into interpretation.
Autonomous Robotics *Nanorobots*	Collaborative robotics (cobots) *Nanocobots*	Industry 4.0: Autonomous robots execute tasks with human intervention. Industry 5.0: Collaborative robots work alongside humans in shared environments, enhancing interaction.
Digital Twins *Virtual model of F110 frigate for predictive maintenance.*	Cognitive digital twins *Digital twin of an F110 frigate with cognitive integration*	Industry 4.0: Simulates physical systems for optimization and prediction. Industry 5.0: Incorporates cognitive and emotional variables, reflecting human impact on processes.
Virtual Reality (VR) *Immersive tactical training for crews.*	Immersive augmented reality *AR system for tactical support and operator resilience.*	Industry 4.0: Trains technical and operational skills. Industry 5.0: Focuses on well-being and psychological resilience, improving human experience.
Cyber-Physical Systems *Integration of sensors and actuators in armored vehicles.*	Resilient socio-technical systems *Adaptive command and control architecture centred on the operator.*	Industry 4.0: Integrates hardware and software for automation. Industry 5.0: Designed for social adaptability, considering diversity and human needs.
Smart Automation *Drone swarms.*	Human-centred automation *Drone swarms with direct human interaction.*	Industry 4.0: Seeks efficiency and cost reduction. Industry 5.0: Respects operator autonomy and dignity, avoiding dehumanization.
Blockchain *Secure record of military logistics chain.*	Sustainable and auditable blockchain *Blockchain platform for ethical traceability in military supplies.*	Industry 4.0: Ensures traceability and security in transactions. Industry 5.0: Optimized for sustainability and ethical governance, reducing environmental impact.
Digital Tactical Simulation	Cognitive simulation focused on well-being	Industry 4.0: Reproduces technical scenarios for testing.

Simulation centre for land combat training.	*Immersive platform for resilient naval crew training*	Industry 5.0: Incorporates human and ethical variables into strategic decision-making.
Advanced Processing *Data centre for operational intelligence analysis*	Advanced quantum computing *Quantum warfare.*	Industry 4.0: Focuses on advanced computing for analysis. Industry 5.0: Includes quantum cryptography and accelerated decisions with a strategic focus.
Bio-inspired and biomimetic sensors *Thermal sensors for environmental monitoring in bases.*	Advanced bio-inspired and biomimetic sensors *Biomimetic sensors for adaptive detection in hostile environments-*	Industry 4.0: Tracks environmental conditions. Industry 5.0: Implements adaptive and resilient detection based on biological models, mimicking nature.
Cybersecurity *Reactive protection system for tactical networks.*	Proactive cybersecurity *Cyber defence platform with predictive AI and autonomous response.*	Industry 4.0: Reactive protection focused on responding to incidents and vulnerabilities. Industry 5.0: Implements predictive and self-adaptive cyber intelligence, anticipating threats and adjusting dynamically.
Communication Networks *Tactical SDR radio.*	6G or ultra-secure communication networks *6G tactical architecture for multi-domain operations.*	Industry 4.0: Fast and stable connectivity for data exchange. Industry 5.0: Resilient, secure communications with human prioritization, ensuring continuity and protection in critical environments.

Source: Own elaboration.

For Spain, the transition towards Defence 5.0 represents a strategic opportunity to consolidate a national innovation ecosystem centred on the human factor. This process requires strengthening collaboration between the Ministry of Defence, universities, technology centres, and companies. Likewise, it is essential to develop sovereign capabilities in critical technologies such as artificial intelligence, cybersecurity, and digital twins, while promoting active participation in European innovation frameworks such as Horizon Europe and the European Defence Fund. All of this must be accompanied by a firm commitment to ensure that technological innovation aligns with democratic values, human rights, and sustainability objectives. In this sense, Defence 5.0 is not merely a technical evolution but a profound institutional transformation that demands a new organizational culture, technology governance, and a long-term strategic vision.

2.3 The Human Component in the Technological Transformation of Defence.

The transition towards Industry 5.0 implies a shift in approach: from digital defence to cognitive and human-centric defence. In the military context, this means moving from automated and connected systems, characteristic of Defence 4.0, to systems that integrate human cognitive capabilities, operational ethics, and collaboration between operators and intelligent machines that, beyond the automated nature of their decisions, demonstrate active engagement in risk assessment, rule application, and decision-making criteria.

Digital defence, based on the principles of Industry 4.0, has enabled significant advances; however, these advances have also generated, as mentioned in previous paragraphs, ethical, strategic, and operational challenges, such as delegating lethal decisions to algorithms, cyber vulnerability, and the need to ensure effective human oversight in highly automated environments. This last aspect is particularly relevant, as the interaction between operators and intelligent systems must be designed to preserve human supervision, legal responsibility, and operational control at all times (Barroso & Pérez, 2025; IEEE, 2020).

Cognitive and human-centric defence proposes a model in which technology adapts to the operator, not the other way around. This approach is based on the recognition that military systems should not only be efficient but also intuitive, safe, and responsible. In this paradigm, the operator is not a mere executor of automated commands but an active agent in decision-making, whose perception, motivation, and resilience are strategic elements. This implies the development of user-centred interfaces, designed under principles of cognitive ergonomics and accessibility, to facilitate smooth interaction between humans and intelligent systems. According to Chaca-Espinoza et al. (2025), integrating AI into user-centred design environments enables the creation of systems that act as cognitive collaborators, capable of adapting to the operator's needs in real time.

Additionally, the use of decision-support systems is promoted, combining natural language processing, predictive analytics, and advanced visualization to assist the operator in highly complex contexts. These systems do not replace human judgment but amplify it, reducing cognitive load and improving operational accuracy. Immersive simulation environments based on augmented reality (AR) allow training of tactical, cognitive, and emotional skills in realistic yet controlled scenarios. Maraggi (2021) highlights that these environments not only improve technical performance but also strengthen the psychological resilience of military personnel in critical situations. Finally, this technological model must respect the fundamental rights of operators, such as privacy, autonomy, and psychological safety. In the military domain, this means ensuring that systems do not violate personal privacy, that automated decisions are auditable, and that prolonged exposure to digital stress environments is avoided.

In this new scenario, defence sector professionals face unprecedented training challenges. The diversity and complexity of technological systems require multidisciplinary profiles capable of operating in highly digitalized environments, with competencies in artificial intelligence, cybersecurity, data analytics, and advanced simulation. This demand transforms traditional criteria for selection, evaluation, and promotion of military personnel, forcing institutions to review their models of training and professional development (Centro Universitario de la Defensa. Academia General Militar, 2022; European Defence Agency, 2021).

This growing reliance on technological solutions in defence is driving a profound transformation in career paths for military and civilian personnel. Technical specialization, the ability to operate complex systems, and familiarity with digital environments are displacing traditional evaluation criteria such as seniority or conventional operational experience. This evolution may generate conformity dynamics, where decision-makers tend to align with options most supported by intelligent systems, to the detriment of singular or disruptive proposals. Algorithms, by assigning greater reliability to solutions that match their reference models, can reinforce this trend, sidelining those that, although innovative, do not fit their prediction patterns (Helbing, 2019; Bryson, 2018). In this context, the value of human uniqueness, intuition, contextual experience, and the ability to think outside established margins risks being overshadowed by the statistical logic of systems, requiring a critical review of professional development and decision-making models in defence.

Finally, the human component introduces unpredictable variables such as subjective risk assessment, contextual understanding of operations, and, ultimately, chance. These factors can challenge the reliability of technological systems and generate tensions between trust in machines and human operator autonomy. In this sense, Defence 5.0 should not be conceived as a replacement for the human being but as a co-evolution where technology enhances—but does not replace—the critical and strategic capacity of people (Floridi et al., 2018; Defence AI Strategy UK, 2022).

3. Overview of Defence 5.0 in Spain

3.1 Innovation Strategy of the Ministry of Defence

The transformation towards Defence 5.0 in Spain requires a solid, coherent innovation strategy aligned with the technological, operational, and ethical challenges of the new model. In this context, the Ministry of Defence has structured its R&D&I policy through the Defence Technology and Innovation Strategy (ETID), which constitutes the main planning and execution instrument for technological innovation actions in the military sphere. The current ETID 2020 is integrated within the Spanish Strategy for Science, Technology and Innovation (EECTI 2021–2027) and the State Plans for Scientific and Technical Research and Innovation, enabling effective coordination between the sectoral priorities of the Ministry of Defence and the general objectives of the national innovation system. Its strategic objectives are structured around three complementary pillars:

- Technological objectives: Direct R&D&I investments towards high-impact technologies that enhance military capabilities, such as artificial intelligence, autonomous systems, digital twins, advanced cybersecurity, and collaborative robotics.
- National and international cooperation: Foster synergies among the Ministry of Defence, the Ministry of Science and Innovation, universities, technology centres, companies, and European bodies such as the European Defence Fund (EDF) and the Horizon Europe program.
- Continuous improvement: Position the Ministry as an innovation catalyst, capable of integrating talent, resources, and capabilities to strengthen the national scientific-technological fabric and ensure the country's strategic autonomy.

The ETID establishes that all innovation actions must be guided by the principles of efficiency, sustainability, resilience, and technological ethics. Within the Defence 5.0 framework, this means that developed solutions must not only be technically advanced but also respect fundamental rights, the well-being of military personnel, and environmental commitments. Furthermore, the importance of multi-level cooperation is emphasized, both nationally and internationally. At the national level, the protocol between the Ministry of Defence and the Ministry of Science and Innovation stands out, enabling coordinated efforts and resource optimization. At the international level, active participation in European consortia, dual-use projects, and shared innovation platforms is promoted. Below is a table with some of the relevant consortia, platforms, and collaborative projects in 2025 in the field of defence innovation, both nationally and internationally, aligned with ETID principles and the Defence 5.0 approach:

Table 2. ETID 2025 Consortia, Platforms, and Collaborative Projects.

Name	Involved Agents	Concept
EDF (European Defence Fund)	European Commission, Member States, companies and R&D centres	Funds collaborative defence projects in Europe, including dual-use technologies, artificial intelligence, cybersecurity, and autonomous systems.
DIANA (Defence Innovation Accelerator for the North Atlantic)	NATO, tech companies, universities	Defence innovation accelerator with local Spanish headquarters in Madrid and León. Promotes disruptive solutions in AI, sensors, biotechnology, and cybersecurity.
FEINDEF Innovation Hub	Ministry of Defence, Industry, universities	National innovation platform connecting public and private stakeholders. In 2025, it has been key to showcasing dual-use technologies and fostering international cooperation.
Rearm Europe Plan / Readiness 2030	European Commission, Member States	Strategic initiative to strengthen the European defence industrial and technological base. Includes joint funding and measures to promote sustainable and ethical innovation.
COINCIDENTE Program	Ministry of Defence, tech companies	Funds R&D projects with dual (civil and military) application. In 2025, new calls have been launched focusing on AI, cybersecurity, and sustainability.
Alhambra Venture – Defence Vertical	Spanish startups, investors, Tecdual	Innovation event where dual-use solutions such as hybrid drones, tactical robots, and cybersecurity platforms were presented.
EDA (European Defence Agency) Cooperative Projects	EU Member States, industry, research centres	Promotes multinational defence projects, including interoperability, sustainability, and technological resilience.

Source: own elaboration.

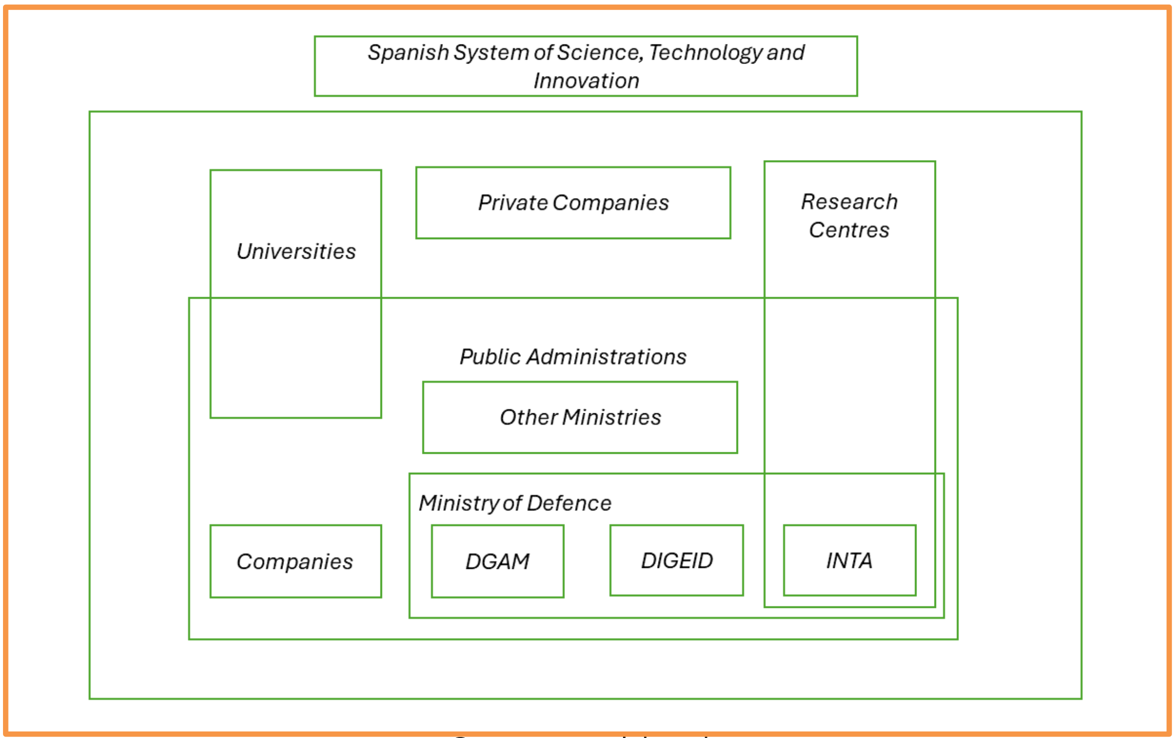
The strategy, in turn, identifies a set of priority R&D&I lines for the 2021–2027 period, which include:

- Autonomous and collaborative systems for multi-domain operations.
- Explainable artificial intelligence applied to command and control, logistics, and cyber defence.
- Cognitive digital twins for simulation, predictive maintenance, and strategic planning.
- Quantum and photonic technologies for secure communications and advanced sensors.
- Collaborative robotics for logistical support, demining, and high-risk tasks.
- Resilient platforms for hostile and high-uncertainty environments.

These capabilities are aligned with the objectives of the National Defence Directive (DDN 2020) and the Defence Policy Directive (DPD 2020), which establish the need to equip the Armed Forces with technological tools that guarantee their freedom of action, interoperability with allies, and responsiveness to emerging threats.

Furthermore, the Ministry of Defence has promoted the creation of a defence innovation ecosystem, which includes the Directorate General for Defence Industry Strategy and Innovation (DIGEID) as the coordinating body for R&D&I, the National Institute for Aerospace Technology (INTA) as the executing agent for technological projects, the Subdirectorate for Planning, Technology and Innovation, responsible for designing and supervising strategic plans, and companies such as ISDEFE, which acts as a bridge between the public and private sectors. This ecosystem is integrated within the Spanish Science, Technology and Innovation System, enabling the use of instruments such as State Research Plans and European funds to finance high-impact projects. Figure 1 illustrates the ecosystem structure.

Figure 1. Defence Innovation Ecosystem and its Integration with the Spanish Science, Technology and Innovation System.



Source: own elaboration.

The Defence Technology and Innovation Strategy (ETID) acknowledges that the transition towards Defence 5.0 is not limited to a mere technological upgrade but represents a profound institutional transformation, requiring a new organizational culture within the Ministry of Defence. In this context, continuous training of military personnel in digital and cognitive skills is promoted to ensure their adaptation to increasingly automated and complex operational environments. Likewise, operator-centred design is encouraged, prioritizing usability, safety, and the physical and psychological well-being of personnel, in line with the principles of Industry 5.0.

Technology governance becomes a fundamental pillar, incorporating mechanisms for human oversight, algorithmic transparency, and data protection, especially in the use of artificial intelligence and autonomous systems. Furthermore, the need to conduct social and environmental impact assessments of technological solutions is established, ensuring that their implementation does not compromise fundamental rights or Spain's environmental commitments. In this regard, ETID is configured as a strategic tool to anticipate the future, build sovereign capabilities, and position Spain as a relevant actor in the European defence and innovation ecosystem, in line with the objectives of the

Spanish Strategy for Science, Technology and Innovation 2021–2027 and the principles of Industry 5.0 (Ministry of Defence, 2020).

3.2 Main Institutional Actors

To implement this strategy, various institutional actors play key roles within the defence innovation ecosystem. The transition towards Defence 5.0 in Spain cannot be understood without the coordinating role of the main institutional actors. These organizations not only execute technological policies but also act as catalysts for the institutional and strategic transformation required by the new paradigm.

In this context, the Directorate General for Defence Industry Strategy and Innovation (DIGEID), the Directorate General for Armament and Material (DGAM), the National Institute for Aerospace Technology (INTA), the public company ISDEFE, and other entities such as CESEDEN and CDTI stand out. Each of them performs specific functions that, together, enable the effective implementation of the Defence Technology and Innovation Strategy (ETID) and the consolidation of a new defence model. Below is a brief explanation of the functions of each of these institutions.

DIGEID, under the State Secretariat for Defence, is responsible for planning and developing the Defence industrial policy, as well as industrial cooperation in this field at both national and international levels. It also leads the implementation of ETID, oversees R&D&I programs, and coordinates collaboration among the various actors in the national science and technology system. Its key functions include:

- Identifying critical capabilities in emerging technologies such as explainable artificial intelligence, collaborative autonomous systems, cognitive digital twins, and advanced robotics.
- Participating in European consortia such as the European Defence Fund (EDF) and the European Defence Agency (EDA), promoting interoperability and strategic autonomy.
- DIGEID also works to foster the creation of collaborative platforms such as the FEINDEF Innovation Hub, which connects companies, startups, universities, and technology centres to accelerate knowledge transfer and promote disruptive innovation.

The Subdirectorate General for Planning, Technology and Innovation within DIGEID is responsible for designing and supervising strategic R&D&I plans in the military domain. Its role is to translate ETID objectives into concrete action lines, coordinating efforts among DGAM, INTA, ISDEFE, and other ecosystem actors. Its functions include:

- Defining technological priorities for the 2021–2027 period, including explainable AI, collaborative robotics, quantum technologies, and resilient platforms.
- Evaluating innovation projects to ensure alignment with principles of sustainability, resilience, and respect for fundamental rights.
- Coordinating with the Spanish Science, Technology and Innovation System, leveraging instruments such as State Research Plans and European funds.

This subdirectorate also promotes continuous training of military personnel in digital, ethical, and cognitive skills, in line with the resilient operator 5.0 model.

DGAM, also under the State Secretariat, is the Ministry of Defence body responsible for planning and developing the Department's armament and material policy, as well as supervising and directing its execution. Through the Subdirectorate General for Armament and Materiel Procurement, it manages the administration and economic and contractual management of research and development programs, as well as acquisition, modernization, and common sustainment programs not included in centralized procurement, for weapons systems and defence equipment, including international cooperation programs. It also handles the management, negotiation, and administration of contracts related to supporting the internationalization of the Spanish defence industry and associated defence material exports.

On the other hand, INTA is the public research organization specialized in aeronautics, space, defence, and security. Its role in Defence 5.0 is fundamental, as it acts as the technical executor of highly complex projects, developing solutions that integrate advanced technologies with ethical and sustainable principles. It also actively participates in European projects and initiatives such as DIANA (Defence Innovation Accelerator for the North Atlantic), promoting disruptive solutions in biotechnology, cybersecurity, and autonomous systems.

The public company ISDEFE, owned by the Ministry of Defence, acts as a strategic and technological consultant in defence, security, space, and transportation projects. In the context of Defence 5.0, ISDEFE serves as a bridge between the public and private sectors, facilitating the integration of innovative solutions into the operational systems of the Armed Forces. Its main contributions include:

- Designing and modelling resilient socio-technical systems that incorporate human, ethical, and environmental variables.
- Consulting on technology governance, especially in algorithm oversight, data protection, and social impact assessment.
- Supporting the Ministry of Defence's digital transformation through the implementation of cognitive platforms, human-centred automation, and immersive simulation.

ISDEFE also contributes to designing safe operational environments, applying principles of cognitive ergonomics and "Hospitality 5.0" to improve military personnel well-being.

An educational and research body is also necessary: CESEDEN. As the Ministry of Defence's strategic think tank, it plays a key role in legal and doctrinal reflection on the application of emerging technologies in the military domain. Within Defence 5.0, its contribution focuses on:

- Analyzing the cognitive implications of military operations, promoting a human-centred approach.
- Developing ethical frameworks for the use of AI and autonomous systems, ensuring human oversight and algorithmic transparency.
- Training in technological leadership and governance for officers and innovation managers.

CESEDEN also fosters a defence culture in society and collaborates with universities and research centres in developing studies and research projects adapted to the new technological paradigm.

Finally, although not directly part of the Ministry of Defence, CDTI is a key actor in financing innovation projects with dual-use applications. Its collaboration with DGAM, DIGEID, and the COINCIDENTE program channels resources to technology companies developing solutions applicable in both civilian and military domains. In the context of Defence 5.0, CDTI:

- Funds deep-tech startups and SMEs working on hybrid drones, cybersecurity platforms, and tactical robotics.

- Promotes technology transfer, facilitating connections between academic research and operational needs.
- Drives the internationalization of Spanish innovation through participation in European programs such as Horizon Europe and EDF.

3.3 Major National Contractors

Companies within the FEINDEF Innovation Hub, such as Indra, Navantia, Airbus Defence and Space Spain, GMV, and Santa Bárbara Sistemas, play a key role in shaping a national defence innovation ecosystem.

Indra positions itself as a leader in intelligent systems and digital defence, structuring its strategy around the digitalization of operational systems, explainable artificial intelligence, and advanced cyber defence. As the industrial coordinator of the FCAS (Future Combat Air System) program, it leads the development of smart sensors, command and control systems, and cognitive simulation platforms. Its commitment to explainable AI enables transparent and auditable operational decisions aligned with ethical principles, while its military cybersecurity solutions integrate predictive analysis, real-time threat detection, and critical infrastructure protection. In terms of sustainability, Indra has incorporated energy efficiency technologies and predictive maintenance, reducing the ecological footprint of military operations, and actively participates in the FEINDEF Innovation Hub, promoting collaboration with startups and universities.

Navantia, the only Spanish company included in the ranking of the world's top 100 defence companies (León et al., 2025), has initiated a profound transformation towards the smart shipyard model, aligned with Industry 5.0 principles. Its participation in the development of the F110 frigates, considered a paradigmatic example of cognitive defence, reflects this evolution. These vessels incorporate digital twins, advanced sensors, collaborative command and control systems, and predictive maintenance platforms, optimizing operational performance and ensuring personnel safety and lifecycle sustainability. Additionally, Navantia has driven the development of unmanned naval platforms, such as surface drones and autonomous submarines, operating in hostile environments under human supervision. These solutions integrate explainable AI, collaborative robotics, and operator-centred design. Organizationally, it has promoted training in digital and cognitive skills and participates in European consortia such as EDF and national initiatives like the COINCIDENTE program.

Airbus Defence and Space Spain is a strategic player in the aerospace and defence sector, with strong involvement in multinational programs and a firm commitment to disruptive innovation. Its participation in FCAS, alongside Indra and other European partners, represents one of the pillars of technological autonomy in defence. It works on developing sixth-generation fighter jets incorporating intelligent UAV swarms, cognitive sensors, explainable AI, and immersive simulation. Additionally, it has developed solutions in secure communications, military satellites, and command and control platforms, integrating quantum, photonic, and contextual processing technologies. Its collaboration with INTA, ISDEFE, and universities, as well as participation in DIANA and EDF, reinforces its commitment to sustainable innovation, complemented by circular economy practices in its industrial processes.

GMV, specialized in systems engineering, cybersecurity, space, and defence, focuses its contribution on developing cognitive platforms, advanced simulation, and adaptive cyber defence. It has worked on projects for modelling and simulating tactical scenarios using augmented reality, digital twins, and machine learning algorithms, training cognitive, emotional, and operational skills in controlled environments. Its AI-based cyber defence systems detect attack patterns, respond autonomously, and ensure human oversight, aligning with principles of algorithmic transparency and technological resilience. In the space sector, it collaborates with INTA and the Spanish Space Agency on observation, navigation, and secure communication satellites and participates in the COINCIDENTE program.

Santa Bárbara Sistemas, a benchmark in land-based weapon systems, has begun its transformation towards Industry 5.0 through process automation, collaborative robotics, and predictive maintenance. Its participation in Army modernization programs and dual innovation initiatives reinforces its strategic role. The company has incorporated digital tools for traceability and efficient management of complex systems and promotes specialized training in technological environments, contributing to operational resilience and national technological sovereignty.

Finally, Escribano Mechanical & Engineering has established itself as a national leader in electro-optical systems, remotely controlled weapon stations, and advanced solutions for land and air defence. Its innovation strategy is oriented towards Industry 5.0, integrating disruptive technologies such as digital twins, collaborative robotics, and predictive cybersecurity into its platforms. The company develops observation and targeting systems incorporating explainable AI, ensuring transparency in critical decision-making and prioritizing operator safety. Additionally, it has promoted resilient and secure connectivity in tactical environments through adaptive networks, reinforcing interoperability with allied systems. In terms of sustainability, Escribano applies predictive maintenance and efficient manufacturing processes, reducing environmental impact and optimizing product lifecycle. Its active participation in the FEINDEF Innovation Hub and collaborative programs with universities and startups demonstrates its commitment to technological sovereignty and the creation of a national defence innovation ecosystem.

3.4 The Role of SMEs and International Collaboration

The transition towards Defence 5.0 in Spain cannot be understood without considering the strategic role played by small and medium-sized enterprises (SMEs) and international collaboration within organizations such as NATO, the European Union, and the European Defence Fund (EDF). These two elements—business fabric and supranational cooperation—constitute fundamental pillars for technological innovation, strategic autonomy, and operational resilience in Spain's defence system.

In the Spanish defence industrial ecosystem, SMEs represent approximately 85% of all companies in the sector, according to Aesmide (2025). This predominance reflects not only their quantitative weight but also their qualitative contribution, as many of these companies lead technological developments in key areas such as artificial intelligence, cybersecurity, robotics, simulation systems, and dual-use technologies (Infodefensa, 2025a). The flexibility, agility, and adaptability of SMEs allow them to respond quickly to emerging technological challenges. For example, companies specializing in software for satellite communications and anti-jamming defence have demonstrated that it is possible to compete in international markets and participate in strategic defence projects with a lean business structure. Many of these companies, originating as university spin-offs or deep-tech ventures, actively contribute to the digital transformation of the military sector, developing solutions that combine operational efficiency with sustainability and technological ethics (Zamora Torralba, 2025).

Moreover, the rise of dual-use technologies has opened new opportunities for SMEs. In sectors such as aerospace, cognitive simulation, or critical infrastructure protection, small companies are developing products that not only strengthen national security but also have a positive impact on the civilian economy (Infodefensa, 2025a).

SME participation in defence has historically been limited by barriers such as regulatory complexity, lack of access to financing, and difficulty integrating into international consortia. However, in recent years, the European Union has implemented specific mechanisms to reverse this situation. The European Defence Fund (EDF), launched in 2021 with a budget of €7.953 billion for the 2021–2027 period, has become the main instrument for promoting collaborative research and development in defence (Zabala Innovation, 2025). The EDF not only funds projects led by major contractors but actively encourages SME and research centre participation through specific calls. In 2025, for example, two non-thematic calls were launched exclusively for innovative SMEs, with funding covering up to 100% of eligible costs. These initiatives aim to accelerate the development of cutting-edge technologies, facilitate prototype validation, and promote cross-border cooperation (Zabala Innovation, 2025).

Spain has positioned itself as one of the most active countries in the EDF, leading 28 of the 91 projects in which it participates and achieving significant economic returns. This leadership has translated into concrete opportunities for national SMEs, which have joined European consortia, scaled their technological solutions, and strengthened their presence in international markets (Infodefensa, 2025a).

Nevertheless, SMEs face significant challenges, particularly in accessing financing. A recent study by the Directorate-General for Defence Industry and Space (DG DEFIS) revealed that 40% of defence-sector SMEs consider it difficult or very difficult to access funding, limiting their growth and participation in strategic projects (European Commission, 2024). To address this gap, the Commission has proposed specific financial instruments, such as venture capital funds and guarantee mechanisms, aimed at encouraging private investment in defence technologies (European Commission, 2025).

In terms of internationalization, the EU has promoted SME participation in cooperation programs with third countries such as South Korea, Japan, Canada, and the United Kingdom through Security and Defence Partnership Agreements. These agreements allow SMEs to access joint tenders, share technical knowledge, and participate in missions under the Common Security and Defence Policy (CSDP) (European External Action Service, 2020; 2018).

3.5 Universities and Public Research Organizations: Knowledge Generators and Strategic Partners in Innovation

The consolidation of a national defence innovation ecosystem requires not only the active participation of the industrial sector but also the strategic involvement of universities and Public Research Organizations (PROs). These institutions play a fundamental role in generating scientific knowledge, developing emerging technologies, and training specialized human capital—key elements for advancing towards a Defence 5.0 model. In this context, collaboration between academia and technology companies accelerates the transfer of research results into operational applications, strengthening technological sovereignty and the country's strategic autonomy.

Spanish universities have intensified their participation in R&D&I projects linked to defence, contributing to the development of critical capabilities such as explainable artificial intelligence, collaborative robotics, cognitive simulation, advanced photonics, and quantum systems applied to multi-domain environments. This contribution goes beyond basic research and extends to applied innovation through prototype creation, proof-of-concept testing, and technological validation in collaboration with companies, including those mentioned in previous sections. Through agreements, university chairs, and joint research centres, stable cooperation channels have been established to align scientific objectives with the strategic needs of the defence sector.

Meanwhile, PROs such as the National Institute for Aerospace Technology (INTA), the Spanish National Research Council (CSIC), and the Centre for Technological Development and Innovation (CDTI) act as innovation catalysts, providing high-level scientific infrastructure, advanced experimentation capabilities, and expertise in international programs. INTA, for example, participates in the development of aerospace technologies, observation satellites, and secure navigation systems in close collaboration with companies and universities. CSIC, with its network of specialized institutes, contributes to advances in smart materials, cognitive sensors, and contextual processing algorithms, while CDTI facilitates the financing of dual-use projects with both civilian and military applications.

These synergies materialize in initiatives such as the programs mentioned in Table 2. Beyond their research role, universities are responsible for training the next generation of professionals in digital, cognitive, and strategic skills essential for operating in increasingly complex and technologically demanding defence environments. The creation of specialized master's and doctoral programs in defence technologies, artificial intelligence, cybersecurity, and autonomous systems, along with the incorporation of dual-use content in technical degrees, helps prepare highly qualified profiles adapted to sector needs.

Overall, the participation of universities and PROs in the defence innovation ecosystem not only strengthens the country's scientific and technological base but also ensures that developments align with ethical principles, sustainability criteria, and national strategic priorities. Their effective integration with the industrial fabric enables progress towards a collaborative and resilient innovation model capable of effectively responding to 21st-century operational challenges.

4. Technologies 5.0 Applied to the Different Defence Subsectors in Spain

4.1 Military Aeronautical Sector

The digital transformation of Spain's military aeronautical sector is driven by the incorporation of 5.0 technologies, which integrate artificial intelligence (AI), advanced connectivity, intelligent automation, and predictive analytics. These technologies not only improve operational efficiency but also strengthen strategic autonomy and responsiveness to emerging threats, redefining both aerial platforms and logistical, maintenance, and tactical operation systems.

Unmanned Aerial Vehicles (UAVs) and Intelligent Swarms

UAVs have evolved from simple reconnaissance tools to key elements of collaborative combat. In Spain, the development of intelligent swarms—groups of UAVs operating in a coordinated manner through AI algorithms—is being promoted by European programs such as the European Defence Fund (EDF) and NGWS/FCAS. In the military domain, UAV swarms enable surveillance, electronic warfare, and attack missions with superior tactical effectiveness. These systems rely on coordination algorithms, autonomous navigation, and real-time communication, allowing them to dynamically adapt to the operational environment (Mohsan et al., 2023).

The incorporation of technologies such as edge computing, distributed artificial intelligence, and inertial navigation systems has enabled UAVs to operate with greater autonomy and precision. In Spain, companies like Airbus and the SIRTAP program are developing tactical UAVs with swarm capabilities for intelligence, surveillance, and reconnaissance missions. Additionally, the concept of intelligent swarms is linked to the use of digital twins, which allow simulating UAV behaviour in virtual environments before real deployment. This technology improves mission planning, route optimization, and energy management for drones (Amjad, 2025). The ability of swarms to execute complex missions—such as autonomous surveillance, electronic warfare, or coordinated attack—relies on deep learning techniques and autonomous decision-making. According to Wang et al. (2024), the use of deep reinforcement learning (DRL) enables UAVs to dynamically adapt to combat environments, optimizing manoeuvres and minimizing operational risks.

Furthermore, the European Union has prioritized the development of unmanned systems as part of its strategic autonomy strategy. The European Defence Agency (EDA) and the European Commission have funded projects integrating UAVs into joint operations, fostering interoperability between platforms and collaboration with NATO (Clapp, 2025).

The FCAS Program and Sixth-Generation Fighters

The FCAS (Future Combat Air System) program, led by France, Germany, and Spain, represents Europe's largest effort to develop a sixth-generation air combat system. This system includes a next-generation fighter (NGF), remote carriers, advanced sensors, and a combat cloud connecting all elements in real time. Spain actively participates in FCAS through companies such as Indra, Airbus DS, ITP Aero, and the Satnus consortium. The program incorporates disruptive technologies such as low observability, human-machine integration, embedded artificial intelligence, and cognitive simulation. FCAS aims not only to replace current Eurofighter and Rafale aircraft but also to establish a new paradigm of collaborative combat (Infodefensa, 2022). Virtual missions conducted in simulators allow evaluation of tactile interfaces, augmented reality, and task allocation to drone swarms, anticipating a revolution in airspace operations (Infodefensa, 2023).

The commitment to an open and modular architecture will allow the integration of future technologies, ensuring system evolution beyond 2040. According to Airbus Defence and Space, FCAS is designed to be scalable, interoperable, and resilient against emerging threats such as hypersonic systems or cyberattacks (Infodefensa, 2022).

Sensors and Radars

Technological evolution in Spain's military aeronautical sector has been marked by the incorporation of 5.0 technologies, particularly in sensor systems, radars, and predictive maintenance. These innovations not only enhance aircraft operational capability but also strengthen security, logistical efficiency, and the strategic autonomy of the national defence system.

Sensors and radars are key elements in surveillance, detection, and response to aerial threats. In recent years, Spain has made significant progress in modernizing its radar systems with solutions such as Lanza-T and Lanza 3D-LRR, developed by Indra. These systems stand out for their ability to detect stealth aircraft, drones, and low radar cross-section (RCS) targets, as well as their resistance to electromagnetic interference and tactical deployment capability (Infodefensa, 2025b,c,d).

The Lanza-T radar, for example, has been integrated into the national Air Defence System and transmits real-time data to the Torrejón command and control centre. Its three-dimensional design and advanced digital processing enable active electronic scanning, improving threat identification accuracy and optimizing performance in complex operational environments (Infodefensa, 2025b). This technology represents a qualitative leap compared to previous systems such as the AN/TPS-43M, offering greater range, energy efficiency, and integration capability with air surveillance networks.

Additionally, the Lanza 3D-LRR radar, deployed at the Villatobas Air Base (Toledo), has been recognized as a milestone in the modernization of the Air Surveillance and Control System (SVICA). Its ability to detect stealth targets and its domestic manufacturing reinforce Spain's technological sovereignty and strategic independence in defence (Infodefensa, 2025c,d).

These technologies are complemented by electronic warfare systems and distributed sensors on interconnected vehicles, capable of creating protective bubbles against drone attacks. The integration of proprietary and third-party sensors into mobile platforms enables dynamic and coordinated responses in high-intensity scenarios, as demonstrated in the development of Tarsis and Valero systems (Infodefensa, 2025e).

Predictive Maintenance Based on Artificial Intelligence

Predictive maintenance is another area where 5.0 technologies are transforming the military aeronautical sector. The application of artificial intelligence (AI) allows anticipating failures, optimizing maintenance cycles, and reducing aircraft downtime. This capability is particularly relevant in demanding operational environments where system availability and reliability are critical. According to the European Union Aviation Safety Agency (EASA), AI applied to maintenance can predict component lifespan, improve logistical planning, and prevent breakdowns through the analysis of large volumes of data generated by onboard sensors (EASA, 2023). This technology detects wear patterns, operational anomalies, and conditions that could compromise system safety or effectiveness.

Advanced models such as CNN-LSTM-Attention have demonstrated high accuracy in predicting the remaining useful life of aircraft engines, enabling informed decisions on component replacement and scheduling technical interventions (Deng & Zhou, 2024). These systems combine convolutional neural networks with attention mechanisms to improve data recognition and prediction reliability.

Moreover, AI facilitates the implementation of maintenance strategies based on the actual condition of equipment rather than fixed schedules. This reduces operating costs and improves safety by preventing unexpected failures. The digitalization of maintenance processes and the integration of intelligent diagnostic systems are being adopted by the Spanish Armed Forces under programs such as the Industrial and Technological Plan for Security and Defence (Ministry of Defence, 2025).

EASA has developed a specific roadmap for AI integration in aviation, including guidelines for machine learning applications in maintenance and flight operations. This roadmap establishes ethical principles, applicability requirements, and certification criteria to ensure that AI-based solutions are safe, reliable, and compliant with European standards (EASA, 2024).

In short, the combination of advanced sensors, smart radars, and AI-based predictive maintenance is redefining Spain’s military aeronautical sector. These technologies not only increase responsiveness to threats but also optimize resource management, reinforce operational safety, and consolidate the country’s technological autonomy in defence.

4.2 Land Sector

The digital transformation of Spain’s land defence sector is driven by the incorporation of 5.0 technologies that redefine mobility, situational awareness, logistics, and crew support. These innovations are being promoted by the Spanish Army in collaboration with the national industry under strategic programs such as the MC3 Plan and the European Defence Fund.

Autonomous Land Vehicles and Collaborative Systems

The use of autonomous land vehicles has moved from a future possibility to an operational reality. At the 2E+I Forum in Toledo, the Spanish Army presented significant advances in the robotization of land platforms, highlighting the role of 5G in interconnecting unmanned systems and integrating them with command and control networks (Infodefensa, 2025f). Companies such as Indra and GMV have developed multipurpose vehicles like the Valero system, designed to operate in collaborative swarms, enabling saturation, deception, and reconnaissance missions without putting crews at risk (Infodefensa, 2025g).

These collaborative systems are based on distributed architectures that allow communication among multiple autonomous units, optimizing real-time decision-making. Artificial intelligence plays a key role in coordinating these vehicles, enabling them to dynamically adapt to the operational environment and respond to emerging threats such as enemy drone swarms (Infodefensa, 2025f,g).

These advances address the challenges faced by the Spanish Army on the modern battlefield, where robotization, anti-drone combat, and technological adaptation are essential to maintain operational superiority (Infodefensa, 2025r).

Augmented Reality and Crew Support

Augmented reality (AR) is revolutionizing crew support on the battlefield. Tools such as XRF.SandBox and XRF.Colossus, developed by the Spanish startup XRF, create precise three-dimensional simulations from satellite images, sensor data, and drones. These platforms offer an immersive experience that improves training, tactical planning, and situational awareness. AR is also being integrated into command and control systems, facilitating real-time visualization of operational data and strategic decision-making. For example, the XRF.Hermes system uses artificial intelligence to interpret complex scenarios and provide recommendations in natural language, acting as a cognitive assistant for military commanders (Infodefensa, 2025h).

Additionally, the European AIDA project, led by Indra, is developing autonomous AI agents that operate in cyberspace and support critical functions such as manoeuvre, fire, sustainment, and protection. These agents not only act autonomously but also assist human operators in decision-making, reducing response cycles and increasing operational effectiveness (Infodefensa, 2025g).

Innovations in Military Land Logistics

Land logistics is another area where 5.0 technologies are having a significant impact. The Spanish Army has launched a contract worth over €1 billion for the acquisition of 4x4, 6x6, and 8x8 tactical trucks to improve mobility, reduce logistical costs, and facilitate maintenance through component commonality (Infodefensa, 2025i). This approach seeks to create a family of vehicles with compatible variants, optimizing the supply chain and streamlining logistical operations in high-demand scenarios. Additionally, capabilities such as unprepared fording in saltwater have been incorporated, expanding vehicle versatility in coastal and amphibious environments.

The European Commission, for its part, has launched the Defence Readiness Omnibus package, which includes measures to accelerate military mobility, simplify procurement processes, and facilitate cross-border cooperation. These initiatives aim to eliminate bottlenecks in the transport of material and personnel and improve the operational readiness of Member States (European Commission, 2025).

Overall, these innovations are redefining Spain's land defence sector, providing greater agility, interoperability, and adaptability. The integration of autonomous vehicles, collaborative systems, augmented reality, and intelligent logistics infrastructures is consolidating a more efficient, resilient, and technologically advanced operational model.

4.3 Naval Sector

The transformation of Spain's naval sector towards a 5.0 model is reflected in the incorporation of technologies such as digital twins, artificial intelligence, autonomous systems, and advanced interconnectivity. These innovations are redefining the design, operation, and maintenance of maritime platforms, consolidating Spain as a benchmark in intelligent naval defence.

Smart Ships and Digital Twin

Navantia, in collaboration with the Spanish Navy, leads the development of smart ships through the Pebba project (Essential Elements of the Autonomous Ship Project). This initiative is based on four strategic pillars: situational awareness, information management, artificial intelligence, and cybersecurity and resilience (Infodefensa, 2025j). The goal is to equip ships with autonomous capabilities that allow them to operate with minimal human intervention, optimizing real-time decision-making.

One of the most disruptive technologies in this field is the digital twin—a virtual replica of the ship that receives real-time data from sensors distributed throughout the vessel. This tool enables monitoring of system status, anticipating failures, and planning maintenance predictively, improving operational efficiency and reducing costs (Infodefensa, 2025j). Additionally, the digital twin facilitates crew training through realistic simulations and contributes to interoperability with other naval platforms.

Navantia has also developed solutions such as Edinaf and the combat cloud, which integrate operational, tactical, and logistical data into a common digital architecture. These technologies strengthen the Navy's operational advantage in complex scenarios where processing speed and adaptability are essential.

Unmanned Naval Platforms

The incorporation of unmanned vehicles in the naval environment has been another key advance. Navantia has designed the Naiad system (Naval Advanced Integrated Autonomous Vehicles Defence System), which enables the control of unmanned aerial vehicles (UAVs), surface vessels (USVs), and underwater vehicles (UUVs) from the ships' combat system consoles (Infodefensa, 2025k). This integration facilitates surveillance, reconnaissance, anti-submarine warfare, and threat neutralization without exposing crews.

The new Maritime Action Ships (BAM) incorporate capabilities to operate with underwater and surface drones, as well as anti-drone systems, 2D exploration radars, ASW decoy launchers, and IRST sensors (Infrared Search and Track). These platforms are designed to effectively respond to current threats through a modular architecture that allows new technologies to be integrated as operational requirements evolve (Infodefensa, 2025k).

Interoperability between manned and unmanned platforms is one of the most relevant technological challenges. Artificial intelligence and machine learning enable coordination of multiple units in real time, optimizing surveillance coverage and threat response. These capabilities are being tested in joint exercises and advanced simulations, with promising results in terms of effectiveness and safety.

F110 Frigates as a Case Study

The F110 program represents the pinnacle of naval technological transformation in Spain. These multi-mission frigates incorporate an unprecedented level of digitalization, including the digital twin, the Integrated Services System, and advanced sensors for anti-air, anti-submarine, and anti-surface defence (Infodefensa, 2025l).

The F110's digital twin allows the crew to access real-time information on equipment status, facilitating operational and maintenance decision-making. The Integrated Services System, developed by Navantia in collaboration with the University of Vigo, acts as the ship's nervous system, with smart nodes managing lighting, public address, wireless connectivity, and CCTV. Additionally, the F110s are equipped with the SPY-7 (V)2 radar, developed by Lockheed Martin, which has demonstrated its ability to track airborne objects in real time during tests at the Aegis-Scomba Integration Centre. This radar, together with the SCOMBA combat system, positions the F110 frigates at the forefront of global naval defence (Infodefensa, 2025m). From an industrial perspective, the F110 program has generated over one million engineering work hours, with companies such as Ghenova developing 80% of the ship's constructive engineering. This effort has consolidated a national technological ecosystem capable of competing in the international market and addressing the challenges of 21st-century maritime defence (Infodefensa, 2025m).

4.4 Defence Consulting and Engineering

Defence consulting and engineering are undergoing a profound transformation thanks to the adoption of 5.0 technologies, which enhance strategic planning, operational decision-making, and logistical efficiency.

Modelling and Simulation in Military Scenarios

Modelling and simulation have become fundamental pillars for designing military operations, training troops, and assessing capabilities. Companies such as Indra have developed centres of excellence dedicated to operational analysis and war games, where tactical, operational, and strategic scenarios are recreated to evaluate the performance of systems and units before deployment (Infodefensa, 2025n). These virtual environments allow simulation of variables such as weather conditions, enemy response, sensor performance, and platform interaction, facilitating informed decision-making and reducing operational risks. Countries like the United States and Israel have demonstrated that such simulations are essential for achieving tactical superiority, and Spain is following this path with initiatives such as the Alcobendas laboratory promoted by Indra (Infodefensa, 2025n).

Additionally, the company XRF has developed extended reality solutions such as XRF.SandBox and XRF.Colossus, which create precise three-dimensional simulations from satellite images, sensor data, and drones. These tools improve situational awareness and geospatial planning and have been recognized by NATO as key technologies in the defence domain (Infodefensa, 2025h).

Digital Twins and Strategic Planning

The use of digital twins in defence enables virtual replication of complex systems such as ships, vehicles, or infrastructures, facilitating monitoring, maintenance, and optimization. Navantia and other leading companies in the sector have applied this technology as mentioned in previous sections. These tools are also being used in mission design, resource management, and industrial capability assessment.

Logistics Optimization through AI and Big Data

Military logistics is being revolutionized by the incorporation of artificial intelligence (AI) and big data. The Ministry of Defence has launched the Numant-IA project, a private and independent data cloud that will manage critical information securely and resiliently. This infrastructure, located in Soria—as its name suggests—will be key to modernizing the Armed Forces' logistical capabilities (Infodefensa, 2025p).

AI enables analysis of large volumes of logistical data to optimize supply routes, predict maintenance needs, and reduce response times. The Prometeo system, deployed by the Spanish Army in Slovakia, allows additive manufacturing of spare parts in operational areas, reducing dependence on external infrastructures and improving self-sufficiency (Infodefensa, 2025q).

Furthermore, the AIDA project, led by Indra, is developing autonomous AI agents capable of operating in cyberspace and supporting critical functions such as sustainment, command, and control. These agents analyze real-time data, detect threats, and provide recommendations, improving logistical efficiency and responsiveness (Infodefensa, 2025f).

Overall, defence consulting and engineering are evolving towards a digital, intelligent, and collaborative model, where simulation, digital twins, and AI enable scenario anticipation, resource optimization, and reinforcement of Spain's strategic autonomy.

4.5 Cybersecurity and Cyber Defence

In today's context, cybersecurity has become an essential component of national defence. Cyber threats in the military domain range from denial-of-service (DDoS) attacks to sophisticated intrusions into command and control systems, digital espionage, and sabotage of critical infrastructures. These threats come not only from state actors but also from terrorist groups and criminal organizations, employing advanced techniques to compromise the security of military systems.

The growing digitalization of the Armed Forces has expanded the attack surface, making weapons systems, communication networks, and logistical platforms vulnerable to cyberattacks. According to Rid (2020), modern conflicts are no longer confined to the physical domain but extend into cyberspace, where operations can have strategic effects without deploying troops.

Artificial Intelligence Applied to Cyber Defence

Artificial intelligence (AI) is transforming the way cyber defence is approached. Machine learning algorithms enable detection of anomalous patterns in large data volumes, identification of emerging threats, and autonomous response to security incidents (Brundage et al., 2018). In the military domain, AI is used to protect networks, analyse vulnerabilities, simulate attacks, and generate real-time tactical recommendations.

One of the most promising applications is the use of autonomous agents operating in cyberspace to perform surveillance, detection, and response tasks. These systems can act without direct human intervention, improving reaction speed against critical threats (Taddeo & Floridi, 2018). Additionally, AI enables cyberattack simulations to train defence teams and assess system resilience.

In Spain, the AIDA project, led by Indra, represents a significant advance in this field by developing intelligent agents capable of supporting command, control, and sustainment functions in complex cyber environments (Infodefensa, 2025g).

Spain's Joint Cyber Command

Spain has consolidated its cyber defence structure with the establishment of the Joint Cyber Space Command (MCCE), created in 2020 as part of the Defence Staff, integrating the Joint Cyber Defence Command (MCCD) created in 2013. Its mission is to ensure the security of the Ministry of Defence's networks and information systems and coordinate military operations in cyberspace (Ministry of Defence, 2023).

The MCCE works in close interaction with national and international organizations, including the National Cryptologic Centre (CCN), NATO, and the European Defence Agency (EDA). It also participates in joint exercises such as Locked Shields, organized by NATO's Cooperative Cyber Defence Centre of Excellence, where large-scale cyberattacks are simulated to assess allied nations' response capabilities (NATO CCDCOE, 2024). Its functions include protecting critical infrastructures, managing cybersecurity incidents, developing offensive and defensive capabilities, and providing specialized training for military personnel. The MCCE also promotes research into emerging technologies such as quantum computing, AI, and digital twins applied to cyber defence. The creation of this command reflects the recognition that cyberspace is an operational domain, just like land, sea, air, and space, in line with NATO's acknowledgment of cyberspace as a domain of operations at the Warsaw Summit in 2016. As Libicki (2007) notes, cyber warfare transcends technical attacks, encompassing a strategic dimension that can alter the balance of power between nations.

4.6 Startups and DeepTech in Defence

In recent years, Spain has experienced significant growth in the innovation ecosystem linked to defence, particularly in the field of technology startups and DeepTech companies. This phenomenon responds to a combination of strategic factors, such as increased investment in military R&D, the promotion of emerging technologies, and the need to strengthen strategic autonomy in an increasingly complex geopolitical context.

DeepTech technologies, characterized by their solid scientific foundation and high disruptive potential, are transforming the defence sector. Areas such as artificial intelligence, quantum computing, advanced robotics, autonomous systems, and cybersecurity are being developed by highly specialized small companies, many of them with dual-use applications suitable for both military and civilian environments (Bonvillian & Weiss, 2015).

This emerging ecosystem thrives on collaboration between startups, universities, technology centres, and major defence companies. The creation of innovation hubs, dedicated incubators, and acceleration programs has enabled new companies to access resources, technological validation, and internationalization opportunities. Furthermore, the growing interest in defence as a strategic sector has fostered the emergence of specialized talent and the transfer of knowledge from academia to industry (Mazzucato, 2013).

Examples of Spanish Startups in Defence and Dual-Use Technologies

Spain has an increasing number of startups developing innovative solutions for the defence sector. Many of these companies work on dual-use technologies, meaning applications for both military and civilian markets, allowing them to diversify and enhance sustainability.

Among the most notable cases are companies working on advanced simulation, extended reality, AI applied to surveillance, autonomous drones, smart sensors, and cybersecurity. These startups have been recognized by international organizations and have participated in joint exercises, specialized fairs, and technology validation programs. For example, some companies have developed three-dimensional simulation systems for military training, using geospatial data and sensors to recreate complex operational environments. Others have created predictive analytics platforms that anticipate threats and optimize real-time decision-making. There are also initiatives focused on additive manufacturing of components, smart logistics, and asset management through IoT technologies. Likewise, although few Spanish companies exist in this niche, technologies for strategic intelligence to support decision-making with dual-use applications—civil and military—are being developed. These solutions not only improve the operational efficiency of the Armed Forces but also strengthen the country's technological resilience. The ability to generate innovation from the national business fabric is key to reducing dependence on external suppliers and ensuring sovereignty in critical areas.

Additionally, the dual-use approach allows these technologies to be applied in sectors such as emergency response, critical infrastructure, public safety, environmental protection, or the energy industry, expanding their social and economic impact. In this sense, defence acts as an innovation catalyst with positive effects across multiple domains. Against this backdrop, it is relevant to analyse comparatively how differences between the 4.0 and 5.0 paradigms manifest in the various defence subsectors: aeronautical, land, naval, consulting and engineering, cybersecurity, and startups and DeepTech. This comparison identifies not only the technologies employed at each stage but also changes in their strategic, ethical, and functional orientation. The following table summarizes this evolution, offering a structured view of the technological tools associated with each paradigm and their sectoral application in the Spanish case.

Table 3. Comparison of Industry 4.0 versus 5.0 by Subsectors. Source: own elaboration

Subsector	Technologies 4.0	Technologies 5.0	Trends 2030 (Opportunities / Challenges / Applications)
Aeronautical	▪ Military Internet of Things (IoBT); ▪ AI; ▪ Big Data for information analysis; ▪ Digital twins; ▪ Automated robotics; ▪ Virtual reality; ▪ Distributed sensors for surveillance, data collection and system control; ▪ Human-machine interfaces; ▪ Tactical simulation.	▪ IoBT focused on human operator, sustainable and resilient; ▪ Explainable AI and joint human-machine decision-making; ▪ Big Data integrated with AI, smart platforms; ▪ Cognitive digital twins; ▪ Intelligent swarms; ▪ Extended reality; ▪ Smart and bio-inspired sensors that adapt to environment and operator; ▪ Operator-centred interfaces; ▪ Immersive cognitive simulation; ▪ Predictive maintenance with AI and digital twins; ▪ Coordinated autonomous operations between manned and unmanned aircraft.	▪ Autonomous operations with AI coordination; ▪ Intelligent predictive maintenance; ▪ Integration of clean energy; ▪ Sustainable autonomous drones.
Land	▪ IoBT; Robotics; ▪ Virtual reality; Sensors; ▪ Tactical simulation; ▪ Digital connectivity; ▪ Automated land vehicles; AI.	▪ IoBT focused on human operator, sustainable and resilient; ▪ Collaborative robotics; ▪ Augmented and extended reality; ▪ Smart and bio-inspired sensors that adapt to environment and operator; Immersive cognitive simulation; ▪ Operator-centred digital connectivity; Autonomous agents; ▪ Smart logistics; ▪ Explainable AI and joint human-machine decision-making.	▪ Adaptive tactical networks; Smart materials; ▪ Sustainable energy for autonomous vehicles; ▪ Edge computing for field control; ▪ AI for predictive tactical decisions.
Naval	▪ IoBT; Automated ships; ▪ Digital twins; ▪ Connected platforms; ▪ Tactical simulation; ▪ AI; ▪ Technical interoperability.	▪ IoBT focused on human operator, sustainable and resilient; ▪ Smart ships; ▪ Cognitive digital twins; Unmanned platforms; ▪ Immersive cognitive simulation; ▪ Explainable AI and joint human-machine decision-making; ▪ Advanced interoperability.	▪ Distributed underwater sensors; ▪ Advanced maritime cybersecurity; ▪ AI for predictive fleet maintenance; ▪ Hybrid autonomous and manned systems; ▪ Distributed ocean intelligence.
Consulting & Engineering	▪ Big Data for data analysis; ▪ Tactical simulation; ▪ Process modeling and automation; ▪ Predictive analysis.	▪ Big Data integrated with AI, smart platforms; ▪ Private data cloud; ▪ Immersive cognitive simulation; ▪ AI for processes (e.g., logistics);	▪ Generative AI for system and scenario design; ▪ Digital twins of complete ecosystems;

Table 3 (cont.). Comparison of Industry 4.0 versus 5.0 by Subsectors. Source: own elaboration

Subsector	Technologies 4.0	Technologies 5.0	Trends 2030 (Opportunities / Challenges / Applications)
Consulting & Engineering	▪ Big Data for data analysis; ▪ Tactical simulation; ▪ Process modeling and automation; ▪ Predictive analysis.	▪ Big Data integrated with AI, smart platforms; ▪ Private data cloud; ▪ Immersive cognitive simulation; ▪ AI for processes (e.g., logistics); ▪ Additive manufacturing; ▪ Digital twins for strategic planning.	▪ Generative AI for system and scenario design; ▪ Digital twins of complete ecosystems; ▪ Expert decision-support systems; ▪ Cognitive automation of defence processes.
Cybersecurity	▪ Detection systems; ▪ Vulnerability analysis; ▪ Network protection; ▪ Attack simulation.	▪ Autonomous detection systems with AI and deep learning; ▪ Predictive and proactive analysis with explainable AI; ▪ Cognitive and adaptive cyber defence; ▪ Immersive cognitive simulation with digital twins and augmented reality; ▪ Autonomous agents; ▪ Cyber resilience.	▪ AI-based threat intelligence; ▪ Active and autonomous cyber defence; ▪ Behavior-based detection; ▪ Quantum security; ▪ Distributed AI for automatic incident response.
Startups & DeepTech	▪ Advanced simulation; ▪ Applied AI; ▪ Smart sensors; ▪ Drones; ▪ Traditional cybersecurity; ▪ Additive manufacturing.	▪ Immersive cognitive simulation; ▪ Explainable AI and joint human-machine decision-making; ▪ Advanced sensors; ▪ Collaborative drones with AI + Edge Computing; ▪ Cognitive and proactive cybersecurity with AI, blockchain and post-quantum cryptography; ▪ Personalized manufacturing with AI + sustainability + digital twins; ▪ Dual-use technologies.	▪ Quantum computing applied to defence; ▪ Civil-defence dual ecosystems; ▪ New technological spin-offs; Open innovation; ▪ New sustainable smart materials.

5. Conclusions

The transition from Industry 4.0 to Defence 5.0 represents a paradigm shift that redefines the role of technology in the military domain, placing human-centricity, sustainability, and resilience at the core of industrial development. This approach does not imply a break with the previous model but rather an evolution that incorporates ethical, social, and environmental principles into the design, implementation, and governance of defence technologies.

For Spain, this process constitutes a strategic opportunity to consolidate a national defence innovation ecosystem capable of generating sovereign, sustainable capabilities aligned with democratic values. Active participation in European programs such as the European Defence Fund (EDF), the FCAS (Future Combat Air System), and NATO's DIANA initiative, together with the strengthening of the Defence Technology and Innovation Strategy (ETID), could position the country on a trajectory of technological leadership. This should be supported by reduced resistance to change, easier access for SMEs, increased public investment, public-private cooperation, and specialized training.

The incorporation of technologies such as explainable artificial intelligence, cognitive digital twins, collaborative robotics, immersive augmented reality, and cognitive platforms not only improves operational efficiency but also promotes a defence model centred on the human operator, where decision-making relies on intuitive, auditable, and adaptive systems. This orientation requires institutions responsible for defence technology development—such as the Ministry of Defence, DGAM, DIGEID, INTA, ISDEFE, and CESEDEN—to adopt an organizational culture that prioritizes technology governance, continuous training in digital and cognitive skills, and design focused on the well-being of military personnel.

In this context, Spanish institutions should strengthen inter-ministerial cooperation and collaboration with the national science and technology system, articulating financing, incubation, and technology transfer mechanisms that integrate SMEs, startups, and deep-tech companies into strategic defence projects. It is also essential to establish clear regulatory frameworks for the responsible use of artificial intelligence, ensure interoperability between legacy and emerging systems, and promote environmental sustainability practices throughout the military industry value chain.

From an academic perspective, this new paradigm opens multiple research lines worth exploring. These include governance models for emerging military technologies, assessment of the environmental impact of technological innovation in defence, operator-centred design from cognitive ergonomics, technological interoperability in multinational scenarios, dual-use innovation and its transfer to the civilian domain, development of autonomous agents for cyber defence, and analysis of the socio-economic impact of Defence 5.0 on employment and national competitiveness.

Ultimately, Defence 5.0 should not be understood as a mere technical evolution but as an institutional transformation requiring a long-term strategic vision, robust ethical governance, and a firm commitment to sustainability, resilience, and human centrality. Spain, as a medium power with a European and Atlantic vocation, has the opportunity to become a benchmark in responsible military innovation—provided it succeeds in articulating its technological capabilities with a defence policy oriented towards social well-being, global security, and strategic autonomy.

In short, Spain faces a decisive juncture: to embrace the transition towards Defence 5.0, aiming to improve its technological, industrial, and military autonomy for the future. This requires a medium- and long-term policy, as it involves not only adopting new technologies but also building an ethical, resilient, and human-centred model capable of projecting its influence within the European and global context.

6. References

Aesmide. (2025). La industria para la Defensa: el papel esencial de las pymes. Aesmide. Disponible en: https://aesmide.es/la-industria-para-la-defensa-el-papel-esencial-de-las-pymes/(Accessed: October 6, 2025)

Amjad, M. (2025). Digital Twin for UAVs: Architecture, Framework, Challenges and Solutions. En Digital Twins for Wireless Networks (pp. 149–159). Springer. https://doi.org/10.1007/978-3-031-73679-7_8.

Atausinchi Masias, A., Atausinchi Masias, D., y Contreras Rivera, R. J. (2025). Ética y sostenibilidad en la innovación tecnológica: revisión sistemática sobre su impacto ambiental. Revista InveCom, 6(1). https://doi.org/10.5281/zenodo.15447180.

Barroso Camiade, C., y Pérez Castrejón, E. M. (2025). Desafíos éticos y legales en el uso de la inteligencia artificial (IA). Sintaxis, (14), 102–118. https://doi.org/10.36105/stx.2025n14.07.

Bonvillian, W. B., y Weiss, C. (2015). Technological Innovation in Legacy Sectors. Oxford University Press.

Carayannis, EG, Morawska-Jancelewicz, J. (2022) El futuro de Europa: Sociedad 5.0 e Industria 5.0 como motores de las futuras universidades.J Knowl Econ, 13, 3445–3471. https://doi.org/10.1007/s13132-021-00854-2

Brundage, M., Avin, S., Clark, J., Toner, H., Eckersley, P., Garfinkel, B., y Amodei, D. (2018). The malicious use of artificial intelligence: Forecasting, prevention, and mitigation. Disponible en: arXiv preprint arXiv:1802.07228. (Accessed: October 10, 2025)

Bryson, J. J. (2018). The Artificial Intelligence of the Ethics of Artificial Intelligence: An Introductory Overview for Law and Regulation. In Proceedings of the 2018 AAAI/ACM Conference on AI, Ethics, and Society. https://doi.org/10.1145/3278721.3278731.

Calderón Leyton, E. (2024). Ética y tecnología: Reflexiones sobre un uso responsable y transformador en América Latina. Revista CUHSO, 34(1). https://doi.org/10.7770/cuhso-v34n1-art662.

Carro Suárez, J., & Sarmiento Paredes, S. (2022). El factor humano y su rol en la transición a Industria 5.0: una revisión sistemática y perspectivas futuras. Entreciencias: Diálogos en la Sociedad del Conocimiento, 10(24), e81727. https://doi.org/10.22201/enesl.20078064e.2022.24.81727.

Castellanos Alba, J. C. (2023). Industria 5.0: un enfoque centrado en el ser humano. Madrid.

Centro Universitario de la Defensa. Academia General Militar. (2022). Innovación docente en la formación universitaria de los oficiales del Ejército de Tierra. Centro Universitario de la Defensa (Zaragoza), Ministerio de Defensa de España. ISBN: 978-84-9091-913-2.

Chaca-Espinoza, W. G., Montenegro-Cajas, P., Ocaña-Parra, S. V., y Medina-Moncayo, A. S. (2025). Integración de Inteligencia Artificial en Design Thinking: Análisis de enfoques para diseño industrial centrado en el usuario. Polo del Conocimiento, 10(6), 1378–1400. https://doi.org/10.23857/pc.v10i6.9720.

Clapp, S. (2025). Military drone systems in the EU and global context: Types, capabilities and regulatory frameworks. European Parliamentary Research Service (EPRS), PE 772.885. Disponible en: https://www.europarl.europa.eu/RegData/etudes/BRIE/2025/772885/EPRS_BRI(2025)772885_EN.pdf. (Accessed: October 10, 2025)

Comisión Europea. (2024). Study results: Access to equity financing for European defence SMEs. DG DEFIS. Disponible en: https://defence-industry-space.ec.europa.eu/study-results-access-equity-financing-european-defence-smes-2024-01-11_en (Accessed: October 6, 2025)

Comisión Europea. (2025). Defence Readiness Omnibus. Defence Industry and Space. Disponible en: https://defence-industry-space.ec.europa.eu/eu-defence-industry/defence-readiness-omnibus_en (Accessed: October 6, 2025)

Comisión Europea. (2025, enero 30). European Defence Fund: Over €1 Billion to Drive Next-Generation Defence Technologies and Innovation. DG DEFIS. Disponible en: https://defence-industry-space.ec.europa.eu/european-defence-fund-over-eu1-billion-drive-next-generation-defence-technologies-and-innovation-2025-01-30_en (Accessed: October 6, 2025)

Corzo-Ussa, G. D., Álvarez-Aros, E. L., & Chavarro-Miranda, F. (2022). La industria 4.0 y sus aplicaciones en el ámbito militar: oportunidad estratégica para Latinoamérica. Revista Científica General José María Córdova, 20(39), 717–736. https://doi.org/10.21830/19006586.882

Deng, S., y Zhou, J. (2024). Prediction of Remaining Useful Life of Aero-engines Based on CNN-LSTM-Attention. International Journal of Computational Intelligence Systems, 17, Article 232. https://doi.org/10.1007/s44196-024-00639-w.

European Union Aviation Safety Agency (EASA). (2023). Artificial Intelligence and Aviation. European Union Aviation Safety Agency. Disponible en: https://www.easa.europa.eu/en/light/topics/artificial-intelligence-and-aviation-0 (Accessed: October 6, 2025)

European Union Aviation Safety Agency (EASA). (2024). Artificial Intelligence Concept Paper Issue 2: Guidance for Level 1 y 2 Machine Learning Applications Disponible en: https://www.easa.europa.eu/en/document-library/general-publications/easa-artificial-intelligence-concept-paper-issue-2 (Accessed: October 6, 2025)

European Defence Agency. (2021). EDA Technology Foresight Exercise – Final Results. Brussels: EDA. Disponible en: https://eda.europa.eu/docs/default-source/eda-publications/edatechnologyforesightexercise-finalresults.pdf (Accessed: October 8, 2025)

Floridi, L., Cowls, J., Beltrametti, M., Chatila, R., Chazerand, P., Dignum, V., ... & Vayena, E. (2018). AI4People—An Ethical Framework for a Good AI Society: Opportunities, Risks, Principles, and Recommendations. Minds and Machines, 28(4), 689–707. https://doi.org/10.1007/s11023-018-9482-5.

Forging Forum. (s.f.). Forging the future of Industry 5.0. Disponible en: https://bridges5-0.eu/forging-a-forum-for-the-future-of-industry-5-0/(Accessed: September 10, 2025)

Foro Transfiere. (s.f.). Foro Transfiere: European Meeting on Science, Technology and Innovation. Disponible en: https://www.forotransfiere.com /(Accessed: September 10, 2025)

Helbing, D. (Ed.). (2019). Towards Digital Enlightenment: Essays on the Dark and Light Sides of the Digital Revolution. Springer International Publishing. https://doi.org/10.1007/978-3-319-90869-4.

Infodefensa. (2022). El FCAS despega por fin: caza europeo del futuro, enjambres de drones y nube de combate. El Debate. Disponible en: https://www.eldebate.com/espana/defensa/20221119/el-fcas-despega-por-fin-caza-europeo-del-futuro-enjambres-de-drones-y-nube-de-combate_73909.html

Infodefensa. (2023). Entendiendo el FCAS: un supercaza, un enjambre de drones y una nube de combate. El Confidencial. Disponible en: https://www.elconfidencial.com/tecnologia/2023-09-07/fcas-supercaza-enjambre-drones-nube-combate_3729940/

Infodefensa. (2025a). Las pymes de defensa piden más protagonismo a la gran industria. Infodefensa. Disponible en: https://www.infodefensa.com/texto-diario/mostrar/5451777/esta-semana-podcast-infodefensa-pymes-defensa-piden-protagonismo-gran-industria (Accessed: September 10, 2025)

Infodefensa. (2025b). El nuevo radar Lanza-T del Ejército del Aire se integra en el sistema de defensa aérea español. Disponible en: https://www.infodefensa.com (Accessed: September 10, 2025)

Infodefensa. (2025c). El Ejército del Aire recibe un radar Lanza-T de Indra capaz de detectar aviones con tecnología 'stealth' y drones. Disponible en: https://www.infodefensa.com (Accessed: September 10, 2025)

Infodefensa. (2025d). El nuevo radar Lanza 3D de vigilancia del Ejército del Aire en Toledo cumple 100 días de operación. Disponible en: https://www.infodefensa.com (Accessed: September 6, 2025)

Infodefensa. (2025e). Así es Valero, el dron multipropósito de bajo coste diseñado por Indra. Disponible en:https://www.infodefensa.com (Accessed: September 6, 2025)

Infodefensa. (2025f). Indra presenta en el Foro 2E+I sus últimos desarrollos en drones, sistemas antidrón y radares de nueva generación. Disponible en: https://www.infodefensa.com (Accessed: September 6, 2025)

Infodefensa. (2025g). Indra lidera el desarrollo de agentes autónomos de IA en apoyo a las operaciones militares en el ciberespacio europeo. Disponible en: https://www.infodefensa.com/texto-diario/mostrar/5297637/indra-lidera-desarrollo-capacidad-central-gestionar-agentes-autonomos-ia-apoyo-operaciones-militares-ciberespacio-europeo (Accessed: September 7, 2025)

Infodefensa. (2025h). La startup canaria XRF se afianza en defensa y entra en el grupo de trabajo de la OTAN de realidad virtual. Disponible en: https://www.infodefensa.com (Accessed: October 6, 2025)

Infodefensa. (2025i). El Ejército de Tierra lanza un megacontrato de 1.000 millones para comprar camiones tácticos 4x4, 6x6 y 8x8. Disponible en: https://www.infodefensa.com (Accessed: October 6, 2025)

Infodefensa. (2025j). Navantia y la Armada avanzan en el desarrollo del buque autónomo. Disponible en: https://www.infodefensa.com/texto-diario/mostrar/5450767/navantia-armada-avanzan-desarrollo-buque-autonomo-proyecto-pebba (Accessed: October 3, 2025)

Infodefensa. (2025k). Las claves de los nuevos BAM de la Armada: misiles antiaéreos, sistema antidrón y preinstalación para sonar. Disponible en: https://www.infodefensa.com/texto-diario/mostrar/5447694/claves-nuevos-bam-armada-misiles-antiaereos-sistema-antidron-preinstalacion-sonar (Accessed: October 3, 2025)

Infodefensa. (2025l). Los hitos del programa F-110 en 2025: botadura de la F-111 después del verano y puesta de quilla de la F-112 en abril. Disponible en: https://www.infodefensa.com/texto-diario/mostrar/5137332/hitos-programa-f-100-2025-botadura-f-111-despues-verano-puesta-quilla-f-112-abril (Accessed: October 3, 2025)

Infodefensa. (2025m). La fragata F-110, el avanzado buque que Navantia quiere exportar. Disponible en: https://www.infodefensa.com/texto-diario/mostrar/5435995/esta-semana-podcast-infodefensa-fragata-f-110-avanzado-buque-navantia-quiere-exportar (Accessed: October 3, 2025)

Infodefensa. (2025n). Indra apuesta por su centro de análisis operacional y juegos de guerra. Infodefensa. Disponible en: https://www.infodefensa.com/texto-diario/mostrar/5423281/reportaje-indra-centro-analisis-operacionalç (Accessed: October 8, 2025)

Infodefensa. (2025p). Defensa invertirá 70 millones en Numant-IA, una nube privada e independiente de datos para las Fuerzas Armadas. Disponible en: https://www.infodefensa.com/texto-diario/mostrar/5414273/defensa-invertira-70-millones-numant-ia-nube-privada-e-independiente-datos-fuerzas-armadas (Accessed: October 8, 2025)

Infodefensa. (2025q). El despliegue español en Eslovaquia, a la vanguardia tecnológica: así fabrica piezas y repuestos en 3D con el sistema Prometeo. Disponible en: https://www.infodefensa.com/texto-diario/mostrar/5405576/despliegue-espanol-eslovaquia-vanguardia-tecnologica-asi-fabrica-piezas-repuestos-3d-sistema-prometeo (Accessed: October 3, 2025)

Infodefensa. (2025r). Los desafíos del Ejército de Tierra en el campo de batalla moderno: de la robotización al combate antidrón. Disponible en: https://www.infodefensa.com (Accessed: October 6, 2025)

Instituto Español de Estudios Estratégicos (IEEE). (2020). Implicaciones del ámbito cognitivo en las Operaciones Militares. CESEDEN.

International Workshop on Industry 5.0 and Society 5.0 (IWIS). (s.f.). Proceedings of the International Workshop on Industry 5.0 and Society 5.0. Disponible en: https://iwis-conference.org (Accessed: September 22, 2025)

Kaswan, M. S., Rathi, R., y Garza-Reyes, J. A. (Eds.). (2023). Industry 5.0: Concepts and Strategies for Digital Transformation. CRC Press.

Kotler, P., Kartajaya, H., y Setiawan, I. (2021). Marketing 5.0: Technology for humanity. John Wiley y Sons.

Leon G.; Gómez Pérez, A.; Dueñas, C.; Álvarez-Gascón, F.; Báez Cristóbal, T.; Gómez de Agreda, A.; Vázquez Martínez, L.; Insenser Farré, J.M.; Morales de los Ríos, J.B.; Ramírez Morán, D., Guerra, L. (2025). Situación y tendencias en al uso de la inteligencia artificial en el sector de la defensa. Foro de Empresas Innovadoras y Amper. ISBN: 978-84-09-75701-5.

Libicki, M. C. (2007). Conquest in cyberspace: National security and information warfare. Cambridge University Press.

Lodeiro Encina, A. (2018). Cuarta Revolución Industrial y sus implicancias en los ámbitos de seguridad y defensa. Cuaderno de Trabajo, 15, Academia Nacional de Estudios Políticos y Estratégicos (ANEPE), Chile.

Maraggi, S. (2021). Entrenamiento Militar en el Continuo de Virtualidad. CEFADigital.

Mazzucato, M. (2013). The Entrepreneurial State: Debunking Public vs. Private Sector Myths. Anthem Press.

Ministerio de Defensa. (2020). Estrategia de Tecnología e Innovación para la Defensa (ETID 2020). Secretaría de Estado de Defensa. Disponible en: https://www.tecnologiaeinnovacion.defensa.gob.es/es-es/estrategia/Paginas/Defensa.aspx (Accessed: September 23, 2025)

Ministerio de Defensa. (2023). Mando Conjunto del Ciberespacio. Disponible en: https://www.defensa.gob.es/organizacion/mando-conjunto-del-ciberespacio/ (Accessed: October 7, 2025)

Ministerio de Defensa de España. (2025). Plan Industrial y Tecnológico para la Seguridad y la Defensa. La Moncloa. Disponible en: https://www.lamoncloa.gob.es/consejodeministros/resumenes/Documents/2025/230425-plan-industrial-y-tecnologico-para-la-seguridad-y-la-defensa.pdf (Accessed: October 8, 2025)

Ministry of Defence. (2022). Defence Artificial Intelligence Strategy. London: UK Government. Disponible en: https://www.gov.uk/government/publications/defence-artificial-intelligence-strategy. (Accessed: October 8, 2025)

Mohsan, S. A., Javaid, N., Saeed, N., Qadir, Z., Fahim, H., He, B., & Song, H. (2023). Communication and control in collaborative UAVs: Recent advances and future trends. arXiv preprint arXiv:2302.12175. https://doi.org/10.48550/arXiv.2302.12175.

NATO CCDCOE. (2024). Locked Shields 2024: World's largest cyber defence exercise. Disponible en: https://ccdcoe.org/exercises/locked-shields/ (Accessed: October 7, 2025)

Pérez-Domínguez, L. A., Ávila-López, J. R., y Luviano-Cruz, D. (2023). Tendencia de la Industria 4.0 comparado con Industria 5.0. Mundo FESC, 13(25), 7–19. https://doi.org/10.61799/2216-0388.1248.

PwC y Siemens. (2025, octubre 7). Claves e inversiones estratégicas para una España 5.0. Expansión. Disponible en: https://www.expansion.com/economia-sostenible/2025/10/07/68e51cf2468aeb0a458b457b.html (Accessed: October 8, 2025)

Rid, T. (2020). Active measures: The secret history of disinformation and political warfare. Farrar, Straus and Giroux.

Riola, J. M., Fajardo-Toro, C. H., Díaz Reina, J., Mayorga Torres, O., y Garnica López, M. A. (2020). Defensa 4.0: Internet de las Cosas en Sistemas de Batalla (IoBT) en Defensa Naval. RISTI-Revista Ibérica de Sistemas e Tecnologías de Información (Edición Especial), 507–519.

Saniuk, S., Grabowska, S., & Adamik, A. (2024). Smart Organizations in Industry 5.0: A Human-centric Approach. Taylor & Francis.

Servicio Europeo de Acción Exterior (EEAS). (2018, marzo 6). Plan de aplicación en el ámbito de la seguridad y la defensa - Factsheet. Disponible en: https://www.eeas.europa.eu/eeas/plan-de-aplicaci%C3%B3n-en-el-%C3%A1mbito-de-la-seguridad-y-la-defensa-factsheet_es (Accessed: October 6, 2025)

Servicio Europeo de Acción Exterior (EEAS). (2020, junio 21). Seguridad y defensa de Europa: el camino a seguir. Disponible en: https://www.eeas.europa.eu/eeas/seguridad-y-defensa-de-europa-el-camino-seguir_es (Accessed: October 6, 2025)

Schwab, K. (2016). The Fourth Industrial Revolution. World Economic Forum

Taddeo, M., y Floridi, L. (2018). How AI can be a force for good. Science, 361(6404), 751-752.

Travez Tipan, A. V., y Villafuerte Garzón, C. M. (2023). Industria 5.0: revisión del pasado y futuro de la producción y la industria. Revista Científica Mundo, 7(1). DOI: 10.37811/cl_rcm.v7i1.4457.

Universidad de los Andes, Colombia (2025). Foro "Personas e industria en la era de la Sociedad 5.0". Disponible en: https://industrial.uniandes.edu.co/es/Foro-Personas-e-Industria-en-la-Era-de-la-Sociedad-5.0 (Accessed: September 6, 2025)

Wang, X., Wang, Y., Su, X., Wang, L., Lu, C., Peng, H., & Liu, J. (2024). Deep reinforcement learning-based air combat maneuver decision-making: Literature review, implementation tutorial and future direction. Artificial Intelligence Review, 57, artículo 1. https://doi.org/10.1007/s10462-023-10620-2.

World Industry 5.0 Forum. (s.f.). World Industry 5.0 Forum. Disponible en: https://www.worldindustry5forum.org (Accessed: September 22, 2025)

Zabala Innovation. (2025, febrero 13). Fondo Europeo de Defensa 2025. Financia tu proyecto. Zabala. Disponible en: https://www.zabala.es/noticias/fondo-europeo-de-defensa-2025/ (Accessed: October 6, 2025)

Zabala Innovation. (2025, marzo 17). Defensa y pymes. Dos convocatorias no temáticas de EDF 2025. Zabala. Disponible en: https://www.zabala.es/noticias/edf-2025/ (Accessed: October 6, 2025)

Zamora Torralba, E. (2025, junio 10). Los pequeños negocios encuentran su hueco en la industria de Defensa. El Economista. Disponible en: https://www.eleconomista.es/economia/noticias/13398992/06/25/los-pequenos-negocios-encuentran-su-hueco-en-la-industria-de-defensa.html (Accessed: October 6, 2025)