ARCHERY
STRATEGY CONSULTING

ARTIFICIAL INTELLIGENCE:

What collaborative model best supports the Armed Forces and the Defense Industrial and Technological Base (DITB)?

November 2024

A. AI OFFERS A MAJOR OPPORTUNITY FOR THE DEFENSE DITB, CREATING A PARADIGM SHIFT IN THE DEFENSE SECTOR

1. AI IS SCALING UP IN THE DEFENSE SECTOR, PROPELLED BY THE PACE OF GLOBAL TECHNOLOGICAL INNOVATION

Artificial Intelligence is already being used in multiple ways within the defense sector, yet its rapid expansion is creating a **significant transformation for the Defense Industrial and Technological Base** (DITB, which includes 9 major groups and 4,500 SMEs in France).

Transitioning from symbolic AI (based on explicit logical rules: equation systems, decision trees, etc.) to **models that can be "implicit"** (statistical learning, neural networks, etc.) and capable of learning, AI now enables systems to perform complex tasks. Through machine learning and deep learning, powered by large annotated datasets, AI can accomplish tasks such as image recognition (computer vision), predictive analysis, and anomaly detection. **Generative AI** goes even further, creating original content and offering new possibilities (design of complex systems, creation of synthetic satellite images, and assisted operational planning).

The development of AI is being driven by **the following key advances**: increased computational power, data abundance (internet, IoT, satellite constellations), increased algorithmic complexity, and miniaturization. Additionally, the rising accessibility of software libraries and cloud computing supports AI model deployment without the need for substantial hardware and development resources.

AI applications for the Armed Forces can be divided into **three main categories: operational AI, embedded AI, and organic AI**. These applications aim to achieve two main goals: to speed up the decision-making process in real-time through optimized processing and enriched data, easing the cognitive burden on operators, and to enhance operational efficiency, especially in mission preparation and operational maintenance.

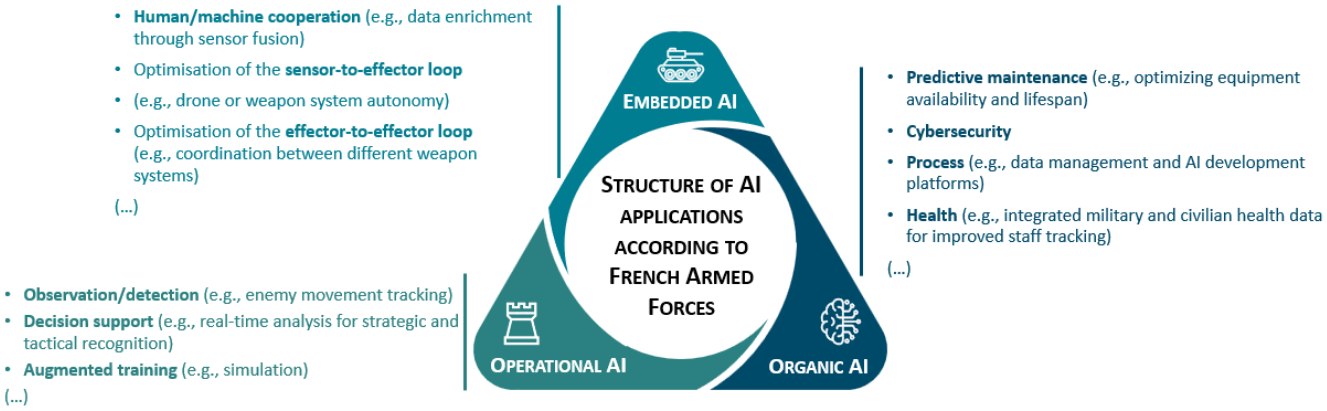

Figure 1: three fields of AI application for the Armed Forces

Fueled by the success of real-life experiments, AI is increasingly integrated into defense ecosystems, especially in embedded and operational AI:

- Ukrainian drones on the battlefield use AI for detecting enemy equipment through computer vision and for automating navigation, targeting, and trajectory adjustments (e.g., Saker Scout drone).
- In the United States, Shield AI has showcased AI's potential in aerial combat, with autonomous F-16 fighters consistently outperforming human pilots in real-world conditions.
- The French DGA (Direction Générale de l'Armement) announced the RBE2 XG radar program for the Rafale in 2023, which will feature AI and an adaptive signal library for learning, identifying, and classifying targets based on their signatures.
- In Europe, AI integration in the Future Combat Air System (FCAS) will allow coordination with autonomous drones carrying payloads (EM jamming, deep strikes), operated by AI models.

The deployment of AI faces several challenges, especially in Europe: defining an ethical framework, addressing biases from technological discrimination that favor or disadvantage certain groups, optimizing AI models to meet efficiency requirements (particularly for embedded AI), and developing reliable AI (valid, robust, ethical, and explainable).

2. AI: A PARADIGM SHIFT RESHAPING THE DEFENSE INDUSTRY ECOSYSTEM

AI serves as a multiplier of effects, allowing systems to handle more information, increase autonomy, and improve accuracy. While hardware ensures mass and availability, **strategic value is increasingly shifting to software and data**, which are becoming the drivers of operational performance.

This evolution has **brought forth new players, who introduce shorter development cycles and more agile methods**. Historically, AI in defense was developed internally by industry players with long project cycles closely aligned with military needs. However, this dynamic has shifted significantly, with the **civilian sector** now leading in technological advancements, particularly in computing power, massive data acquisition, and machine learning. Civilian initiatives like OpenAI (ChatGPT) have demonstrated the potential of generative AI, reshaping the tech ecosystem and shifting roles.

Additionally, the entry of **new players**, such as Helsing, Anduril, and Shield AI, along with tech giants like Google, Microsoft, and Palantir (involved in Project Maven, a Pentagon program for AI drone video analysis), contributes to the rise of a true "**DefTech**" (Defense Technology), encompassing cutting-edge technologies applied to defense and security, such as AI, cybersecurity, and drones. This phenomenon, initially observed in the United States, is gradually gaining traction in Europe, where a similar ecosystem is developing.

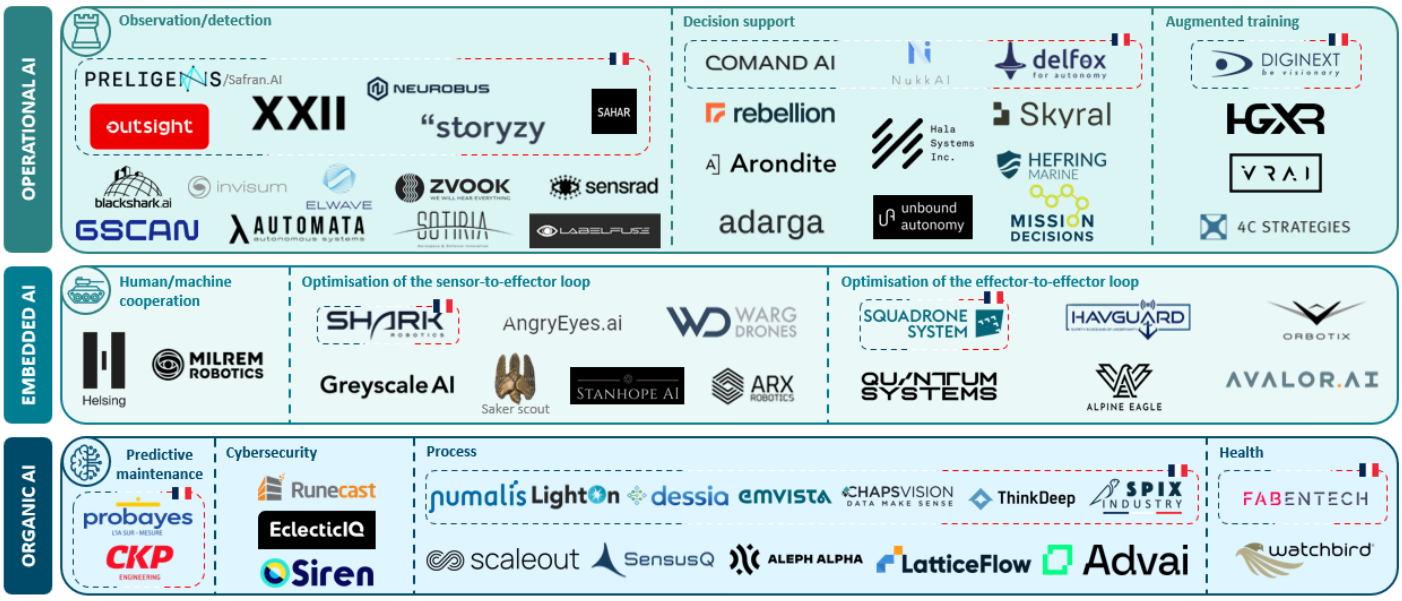

Figure 2: mapping of European start-up/scale-up for AI in defense (DefTech)

The traditional players in the Defense Industrial and Technological Base (DITB) must now align their development cycles with those of agile actors, or risk losing the value of innovation, especially in a context where Concepts of Operations (ConOps) are still largely undefined and evolving rapidly, along with associated technologies. By remaining focused on hardware, these industries risk **losing control over the high added-value segment**, which is essential in modern defense. Those who manage to position themselves quickly in AI will gain a significant strategic edge.

B. CONFRONTED WITH THE PARADIGM SHIFT DRIVEN BY AI, THE DITB AND THE ARMED FORCES MUST OVERCOME SEVERAL CHALLENGES

1. IMPROVING DATA ACCESSIBILITY

The effectiveness of AI models largely depends on their capacity to learn from strong and weak signals (also called "patterns") within large volumes of data, or, in other words, their "experience": the richer and more varied the training data, the better these models can recognize patterns, make autonomous decisions, and adapt to complex situations. For applications like automatic detection of military objects in satellite images, training a model effectively may require millions of images. Furthermore, objects of interest in the military field are constantly evolving (new models, variants, camouflage, etc.), making it essential to continuously supply updated data.

The growing demand for data is further intensified by the proliferation of sophisticated sensors on military platforms. For instance, deep-sea surveillance (Seabed warfare) could generate 1 terabyte every 1.5 hours, while a battalion upgraded to the Scorpion standard might produce up to 30 terabytes per day.

This **"data tsunami"** reaches its peak on a warship equipped with numerous sophisticated sensors (radar, sonar, electronic warfare, optronics, etc.), capturing underwater, surface, and aerial data. This massive volume poses a significant challenge for the Armed Forces, which lack adequate storage, processing, and analysis capabilities, thus limiting the effective exploitation of this information. The creation of the Marine Data and Artificial Intelligence Services Center (CSDIA-M) in Toulon demonstrates the French Navy's awareness of these issues, but it also raises questions about data sharing.

Data sharing in the defense sector remains a sensitive issue. The Armed Forces, concerned about protecting their information and avoiding any leaks, restrict access to external actors. For DITB companies, although they master the equipment and can generate training data under near-real conditions (such as Elbit, which uses its own airborne systems to produce images from its optics), they are reluctant to share it, viewing it as a crucial competitive advantage. While these hesitations are partly legitimate, they nevertheless slow down new AI actors, as synthetic data alone is insufficient to develop innovative solutions and to accelerate the integration of AI in defense.

Collecting, storing, sorting, annotating, correlating, and exploiting data: mastering this chain is essential to ensure not only technological sovereignty but also the operational effectiveness of the Armed Forces against constantly evolving threats. In response to these challenges, the French Ministry of Defense's AI Agency (**Amiad**) was established in March 2024, aiming to bring together 300 specialists by 2026 with an annual budget of 300 million euros. It centralizes data, expertise, and infrastructure (including a classified supercomputer, the most powerful in Europe dedicated to AI). This agency will ensure sovereign data management, establish standards for secure collaborations, and accelerate the development of AI solutions for the Armed Forces, thereby strengthening technological sovereignty and defining a national AI doctrine in defense.

2. Adapting the organizational structure to integrate AI and associated skills

Faced with the rapid pace of innovation, the new dynamics of the defense ecosystem require a reevaluation of the **proprietary development model of the DITB**. However, some industrial players, deeply rooted in their domain expertise, are reluctant to collaborate with DefTech startups, fearing that such collaborations without equity links could serve as a Trojan horse, lowering barriers to entry and promoting the rise of AI-driven competitors, in addition to traditional industrial rivals.

In response, an increasing number of industrial players are opting for **equity partnerships and acquisitions**: this allows them to accelerate the integration of critical AI technologies while maintaining control over intellectual property. For instance, Safran acquired Preligens to anchor its AI strategy, and Saab invested in Helsing, forming a strategic partnership to equip the Luftwaffe's Eurofighter with AI-based electronic warfare capabilities.

This is not the only approach: other major DITB players, such as MBDA and Thales, prefer **creating subsidiaries or dedicated entities** (respectively NEODE Systems and CortAIx) to increase their agility. This enables them to concentrate talent, pool AI knowledge, and accelerate the development of innovative solutions and the cross-functional dissemination of innovations within these groups. By breaking free from the rigid traditional processes of the defense industry, these structures promote greater responsiveness and a faster ability to experiment with emerging technologies.

Building an internal AI technology core ("Make") should not be the only strategic focus for industrial players; acquiring ("Buy") **civilian technological components** is equally crucial to keep pace with rapid innovation, including with solutions that set market standards (such as the LLMs developed by French company Mistral AI). However, this approach raises significant issues of sovereignty, cybersecurity, and confidentiality, while increasing dependence on civilian suppliers: these solutions are therefore mainly adopted for processes rather than critical functions.

3. Adopting more open and collaborative software development models

To address these challenges and facilitate the rapid integration of civilian technologies, adopting an **open architecture** appears to be a preferred approach. Unlike closed systems, these architectures allow for easy addition of new civilian technological components, such as AI, while enhancing interoperability and reducing both costs and timelines. For example, Parrot compensates for its R&D limitations through one of the most active open-source software libraries in the world (ANAFI software development kit). In the United States, the MOSA (Modular Open Systems Approach) model ensures flexibility and interoperability, while limiting dependency on single suppliers, fostering smoother collaboration between the Armed Forces and industrials for accelerated technology adoption.

Adopting an agile approach also requires redefining the role of the Armed Forces in system development: rather than following a rigid V-cycle, they must shift to an **incremental and iterative approach**, with continuous adjustments based on feedback. This requires closer involvement by the Armed Forces and more flexible specifications that can quickly adapt to technological advances, far from the fixed requirements of the traditional model. This iterative approach also helps reduce the time needed for AI technology integration into military operations ("Time to Market") to enable real-life experiments.

4. Redefining the approach to financing and risk-sharing

The growing importance of software and data capabilities requires **substantial investments**: computing infrastructure (either proprietary servers or cloud computing), acquisition of specific datasets, software development, etc. These efforts are crucial to remain competitive with technologically advanced countries like the United States or Israel. Additionally, AI investment remains significant not only initially but throughout the systems' lifecycle, due to ongoing maintenance and upgrade needs. As a result, the cost model is progressively shifting from a CAPEX-intensive model (capital expenditures) to one that **increasingly emphasizes OPEX** (operational expenditures). Industrial players must therefore meet the challenge of rapid innovation while balancing high costs and investment risks, with returns on investment that may take time to materialize.

The financing of these investments by the French government remains a significant challenge. While the Military Programming Law (LPM) and the France 2030 plan allocate substantial budgets, **public budget constraints** greatly limit flexibility. Defense budgets are often reduced by other national priorities, such as controlling the public deficit, and by **internal budgetary trade-offs**, even within the Ministry of the Armed Forces (between programs like the PANG, SNLE 3G, FCAS, or RAFALE). This creates continuous pressure on innovation investments, despite the allocated funds.

In this constrained budgetary context, the acquisition cycles of major defense programs, where **planned innovation** follows precise technological roadmaps to ensure equipment robustness and security, complicate the dynamic allocation of resources. It becomes difficult to integrate **open innovation**, often driven by startups testing emerging solutions like AI, which may be uncertain or unknown at the time of funding allocation. Balancing planned innovation with open innovation, despite the risks, is crucial for driving significant industrial and technological progress.

Given the challenges faced by the state and the Armed Forces in allocating budgets for open innovation and fostering AI champions, the private sector has a crucial role to play. Historically reluctant to invest in defense technologies, viewed as risky or long-term, **private investors** are beginning to reconsider their stance, particularly regarding AI and software applications. The Ukrainian conflict has lifted many moral barriers to investment in this sector, and defense is now an industrial priority for the European Commission. Deals like Safran's acquisition of Preligens also provide more reassuring exit opportunities. This shift could encourage a larger inflow of **venture capital** into DefTech, following the American models of Anduril and Shield AI, which enjoy significant funding through public-private partnerships.

CONCLUSION

Artificial intelligence represents a true disruption for the Armed Forces, offering significant opportunities as well as a relegation risk for the DITB. Despite initiatives already launched, such as the mobilization of resources by industrial players and the creation of Amiad by the French Ministry of the Armed Forces, there is still a **lack of overall coherence and maturity** in collaborative approaches to fully leverage AI's potential.

To overcome these challenges, the **DITB and the Armed Forces must focus their efforts on several strategic areas**: improving data accessibility, adapting the organizational structure to integrate AI and associated skills, adopting more open and collaborative software development models, and redefining the approach to financing and risk-sharing.

The ability to adapt quickly will determine not only the competitiveness of French and European players but also their long-term technological sovereignty in a sector undergoing significant transformation.

Guillaume Boutillot
Partner

Antoine Kimmel
Partner

Emmanuel Miremont
Senior Project Manager

CONTACT

ARCHERY STRATEGY CONSULTING
Paris – Toulouse – Tours – Frankfurt – Singapore
www.archeryconsulting.com

Paris Office
14 rue La Boétie
75008 Paris
Tél. +33 (0)1 84 17 02 75

Toulouse Office
9bis Rue de la Colombette
31000 Toulouse
Tél. +33 (0)7 78 41 20 05

Archery Data&Analytics
1 Boulevard Heurteloup
37000 Tours
Tél. +33 (0)6 17 25 01 43

Frankfurt Office
Thurn-und-Taxis-Platz 6
60313 Frankfurt am Main
Tél. +49 (0)151 1965 9269

PVD Singapore
8 Burn Road #08-02/03
Singapore 369977
Tél. +65 9061 1637

ARCHERY
STRATEGY CONSULTING