

# A Winding Road Before Scaling-Up?

## Defense AI in France

Kévin Martin and Lucie Liversain

DAIO Study 23|17

Ein Projekt im Rahmen von

 **dtec.bw**  
Zentrum für Digitalisierungs- und  
Technologieforschung der Bundeswehr



### **About the Defense AI Observatory**

The Defense AI Observatory (DAIO) at the Helmut Schmidt University in Hamburg monitors and analyzes the use of artificial intelligence by armed forces. DAIO comprises three interrelated work streams:

- Culture, concept development, and organizational transformation in the context of military innovation
- Current and future conflict pictures, conflict dynamics, and operational experience, especially related to the use of emerging technologies
- Defense industrial dynamics with a particular focus on the impact of emerging technologies on the nature and character of techno-industrial ecosystems

DAIO is an integral element of GhostPlay, a capability and technology development project for concept-driven and AI-enhanced defense decision-making in support of fast-paced defense operations. GhostPlay is funded by the Center for Digital and Technology Research of the German Bundeswehr (dtec.bw). dtec.bw is funded by the European Union – NextGenerationEU.

Ein Projekt im Rahmen von



# A Winding Road Before Scaling-Up?

**Defence AI in France**

Kévin Martin and Lucie Liversain

DAIO Study 23|17

Ein Projekt im Rahmen von

 **dtec.bw**  
Zentrum für Digitalisierungs- und  
Technologieforschung der Bundeswehr



## **About the Authors**

Kévin Martin has been a research fellow at the Fondation pour la Recherche Stratégique since 2012 specializing in the analysis of industrial strategies and defense industrial and technological bases (DITBs). He won the French Air Force's René Mouchotte prize in 2013. His research focuses on the French defense industry, the impact of new digital technologies on the defense industrial and technology base (organization, players, changing landscape, etc.), and the impact of emerging defense exporters such as South Korea, Turkey, Brazil, and Singapore on the international arms market. He is also responsible for the "French defense industries" and "Emerging DTIB (Defense Technological and Industrial Base)" modules in the Paris Sorbonne Continuing Education Program (FCPS) Defense Industries and Markets. His X/Twitter account is @kmartin\_FRS.

Lucie Liversain is a PhD student at Ecole Polytechnique's Management Research Center (I<sup>3</sup>-CRG\*). Her work in collaboration with the Interdisciplinary Center of Defense and Security Studies (CIEDS) has led her to delve into the heart of tech ventures looking to scale up their dual use technology in the defense sector. She is currently investigating how deep tech ventures make the tricky transition from exploration to profitable and full-scale exploitation of their technology, based on case studies, including those in the defense sector. Her X/ Twitter account is @LLiversain.

## **Acknowledgments**

The authors thank Dr. Heiko Borchert, Torben Schütz, and Joseph Verbovsky for their valuable comments and suggestions. The authors are solely responsible for any errors in fact, analysis, or omission.

## **Design**

Almasy Information Design Thinking

## **Imprint**

Kévin Martin and Lucie Liversain, *A Winding Road Before Scaling-Up? Defense AI in France*. DAIO Study 23/17 (Hamburg: Defense AI Observatory, 2023)

Defense AI Observatory | Chair of Political Theory | Helmut Schmidt University  
Holstenhofweg 85 | 22043 Hamburg | T +49 40 6541 2776  
www.defenseai.eu | contact@defenseai.eu | @Defense\_AIO

ISSN (online): 2749-5337

ISSN (print): 2749-5345

# Content

1 Summary .....	6
2 Thinking about Defense AI .....	8
2.1 A National Strategic Vision Including Defense .....	9
2.2 The Challenges of Defense AI .....	10
3 Developing Defense AI .....	15
3.3 France's AI Innovation Base .....	16
3.4 Adaptation of France's Traditional Defense Players .....	19
3.5 Defense AI R&D Strategy .....	23
3.6 Priority Application Areas .....	23
3.7 ARTEMIS.IA: Ambition and Reality of Building a Defense AI Ecosystem .....	25
4 Organizing Defense AI .....	28
4.1 Defense AI Governance .....	29
4.2 Data Governance and Data Sharing: A Policy Yet to be Confirmed .....	29
5 Funding Defense AI .....	32
6 Fielding and Operating Defense AI .....	35
6.1 A Wide Range of Initiatives .....	36
6.2 Development through Experimentation: A New Approach to Deploy AI Solutions .....	38
7 Training for Defense AI .....	42
8 Conclusion .....	44
Literature .....	47

# 1 Summary

The French Armed Forces treat artificial intelligence (AI) as a disruptive innovation. AI influences belligerents' behavior by accelerating operational pace across multiple domains, thereby creating a combat environment of several simultaneous confrontations. Since the mid-2010s, AI development is progressing more rapidly thanks to advances in deep neural networks, distributed computing, and increased computing capacity.

France recognized the importance of AI in 2017 when it launched a national strategy to become a world leader in AI. The French Ministry of the Armed Forces published the strategy "AI in service of defense" in 2019, outlining ethical frameworks, infrastructure development, research priorities, and international collaboration. This strategy aimed to create trustworthy AI for defense applications while also embracing dual-use advances on AI in the commercial sector.

The first phase of this strategy saw the construction of a sovereign AI ecosystem focused on research and innovation. This ecosystem established connections between the French Ministry of the Armed Forces, research institutions (INRIA, CEA, CNRS, etc.), traditional defense prime contractors (Thales, Airbus, Dassault Aviation, Safran, MBDA, Naval Group, NExter/KNDS) and non-traditional defense contractors such as AI ventures and SMEs. The second phase, launched in 2022, currently focuses on accelerating AI's integration into key application areas such as decision support, collaborative combat, cybersecurity, logistics, intelligence, and robotics.

France's major procurement efforts, AI studies and research (such as the ARTEMES.IA Program) are earmarked with an average budget of €100M/year. These initiatives seek to harness AI for massive data processing and build a sovereign solution for operational data. But these efforts have faced challenges in integrating non-traditional defense players, aligning timeframes, and addressing varying levels of end-user maturity.

The Armed Forces Ministry is particularly conscious of the ethical and legal issues that may be raised by AI in defense applications. A permanent multidisciplinary ethics committee has been established at the ministry level for emerging technologies in defense. It has already published reports on the use of AI in critical systems.

The French Armed Forces have undertaken various initiatives to integrate and operationalize AI technologies through experimentation. These initiatives aim to help gain operational efficiency and performance, as well as support future organizational change. They explore the challenges of integrating AI on the battlefield, along with accelerating innovation through experimental labs, and co-innovation projects between startups and end-users. Nevertheless, one of the major obstacles to the operationalization of AI in the Armed Forces is the human resource challenge: the ability to attract and retain sufficient AI talent.

Considering the current state of the French defense AI ecosystem, it is possible to imagine several avenues of improvement. These could include supporting efforts to raise awareness for AI investments within defense programs, increasing funding capacities to scale up AI development and a higher R&T budget to fund defense applications of emerging civilian technologies. Finally, it would be possible to facilitate agile co-development between the Armed Forces and industry to build solutions rapidly in response to use cases.

# 2 Thinking about Defense AI

## 2.1 A National Strategic Vision Including Defense

The development of AI accelerated worldwide in the mid-2010s, mainly due to related advances in deep neural networks, optimized distributed computing, and the increase in available computing capacity. This new wave of technology has seen the deployment of the first commercial solutions by major digital players, particularly from the United States. Questions related to its impact on the evolution of digital value chains and on the growth of the sector's economic weight have led many countries to reflect on the issue.

France is no exception. French authorities already fully embraced the topic of AI in 2017. After launching #FranceIA in January 2017, the Prime Minister appointed Cédric Villani,<sup>1</sup> a scientist and newly elected deputy, to head a parliamentary commission. In March 2018, the commission published its report "For a meaningful artificial intelligence: towards a French and European strategy."<sup>2</sup> Using the report as a basis, French President Emmanuel Macron announced the launch of a dedicated national strategy on 29 March 2018, aimed at making France (and Europe) a leader in AI.<sup>3</sup> The strategy primarily focused on France's research sector, one of France's main strengths and considered to be among the global benchmarks in the field.

While emphasizing research, the preparatory report for the national strategy clearly identified defense as one of the sectors in which the development and deployment of AI should play a key role. "AI in support of Defense,"<sup>4</sup> published in September 2019, constitutes the strategy of the Ministry of the Armed Forces (henceforth the French MoD) for AI, providing an ambitious roadmap around six themes:

- Establish a robust ethical and legal framework for the use of AI
- Develop the infrastructure needed to deploy AI
- Define priority research areas
- Establish an AI governance framework
- Innovation, Research and Development Strategy
- International collaboration and export strategy

In addition, the strategy set out the broad outlines of a ministerial policy in this area, based on three pillars:

- Governance: Formalization of a strategic-level departmental data policy, organization and distribution of data-related responsibilities, management of roadmaps

---

1 Philippe, "Mission letter from the French Prime Minister to Cédric Villani."

2 Villani, *For a meaningful artificial intelligence: towards a French and European strategy*.

3 Speech by French President Emmanuel Macron #Aiforhumanity.

4 *AI in Support of Defense*.

- Architecture: Adoption of specific solutions adapted to the constraints of the Armed Forces in the context of data storage, collection, processing, and exploitation
- Culture: Continuous and/or specific training in the use of AI and its challenges, recruitment of specialized personnel

Finally, the key objective of this strategy is to develop trusted AI that meets the unique and strict requirements of the defense world.

## 2.2 The Challenges of Defense AI

The rise of AI not only accelerates defense developments, but it also takes place against the backdrop of intense global competition. The French Armed Forces do not wish to miss out on developments in AI that primarily derive from the commercial sector. As a result, the French Armed Forces dedicated efforts to define a strategy adapted to the constraints and specificities of the defense sector. This strategy is based on two main lines of effort:

- Integrating new technologies, mainly from the civilian sector
- Adapting doctrines and operational concepts to the issues raised by automation, with particular attention to issues of command responsibility.

### A Defense AI Strategy Geared Towards Interaction with the Civilian World

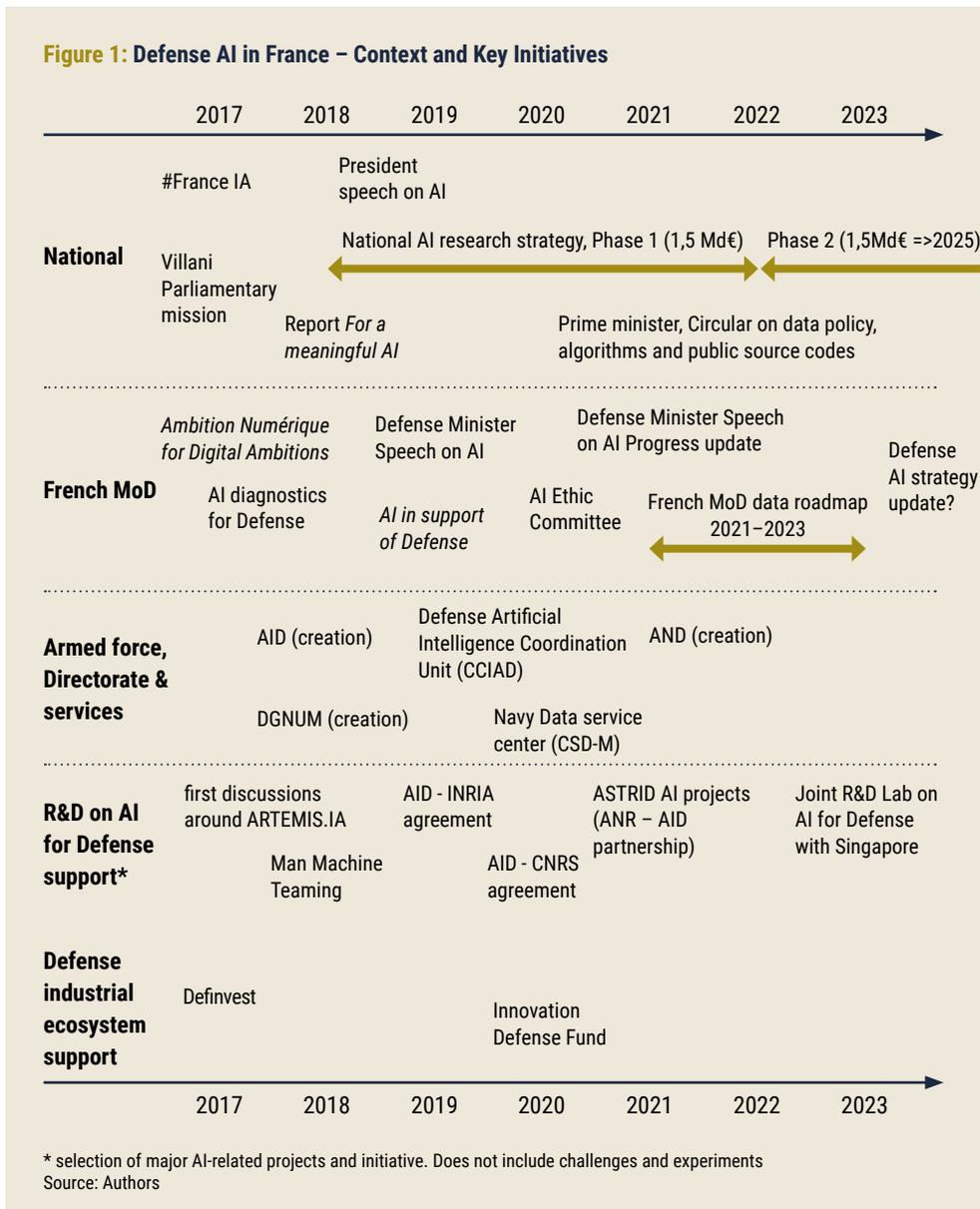
The work on defense AI is part of a global review of the French MoD's strategy, aimed at adapting its structure to the accelerating technological cycles coming from the civilian world. Here the focus is on digital technologies (cybersecurity, cloud computing, AI, semiconductors, quantum computing, etc.), as well robotics, energy, and many others (Figure 1).

Digital innovation, including AI, is enabling spin-in technology transfers, i.e., the capture of innovations developed in a civilian context for integration into a defense system. This is a major paradigm shift after a long period in which spin-out transfers tended to benefit national economies (GPS, radar, etc.). Consequently, the French General Directorate for Armament (DGA), which constitutes France's defense planning and procurement authority, set up the new Defense Innovation Agency (AID) in September 2018. AID's mission is four-fold:

- Lead and drive defense innovation
- Stimulate and capture innovation from the non-defense civilian world

- Improve, transfer and accelerate innovation for the benefit of the Department's users and warfighters
- Identify and implement an innovation approach to prevent strategic surprise

AI is naturally one of the agency's technological priorities.



## Adapting AI to Defense Constraints

While opening to the civilian world seems inevitable, the establishment of a cognitive framework adapted to the requirements of the defense sector remains paramount. This is particularly vital given that while there are many opportunities for the use of AI applications in defense, their level of integration and maturity remains highly variable.

Elementary applications such as automatic classification and object recognition, that have matured in the civilian world, are now fully integrated into the military domain. However, this is not always true for “functional” or even “system”-level applications. The latter are still at an early stage of technological maturity (e.g., autonomous robots capable of sensing and performing multiple tasks in an uncertain environment).

The timing of technological developments is also tied to the changing nature of conflicts. The move towards high-intensity conflict, with battlefield robotization, AI integration, data/sensor fusion, and the quest to saturate the battlefield through mass effect, have all guided defense technology development in recent years. This applies both to the launch of the latest major multi-application projects (Man Machine Teaming, ARTEMIS.IA, etc.) as well as to programs started prior to the launch of the defense AI strategy (Scorpion,<sup>5</sup> Rafale F4,<sup>6</sup> SAIM<sup>7</sup> and SLAMF<sup>8</sup>).

These initial efforts and development projects served as a keystone for a national AI defense strategy. Several key success factors were identified:

- The need to increase the maturity and robustness of technologies for critical applications.
- The availability and accessibility of data needed to explore use cases.
- Infrastructure for AI development, such as clouds. As cloud outsourcing presents a risk to the confidentiality, integrity and availability of data, sovereign combat cloud projects are underway within the French Armed Forces, such as within the new generations of air (SCAF/FCAS) and land (SCORPION) programs. Additionally, the digital transformation of the Armed Forces follows a process launched several years ago and formalized in 2017 with the publica-

---

5 The SCORPION program (standing for synergy of contact reinforced by versatility and network-enabled capability) renews the Army's contact combat through new generation armored vehicles, modernized equipment and a new information system optimizing the networking of systems.

6 The Rafale is a twin-jet fighter aircraft able to operate from both an aircraft carrier and a shore base to carry out all combat aviation missions. Capabilities are developed incrementally and released in packages (“standards”). The first Standard F4 Rafale fighters were delivered to both the French Air and Space Force and to the French Navy in early 2023.

7 The SAIM platform is designed to digitally process real-time data feeds from all types of sensors – satellite, airborne, deployed on the ground – using advanced processing tools to address issues arising from the volume of data and diversity of sources.

8 Future Mine Countermeasures System (SLAMF – Système de lutte anti-mines futur) with autonomous underwater vehicles and unmanned surface vehicles, deployed from a land-based operations center or a mine warfare vessel at sea.

tion of the strategic document “Ambition Numérique for Digital Ambitions” by the French MoD.<sup>9</sup>

- The ability to adapt the workforce (recruitment, profile) of the defense ecosystem to not only develop innovative AI-based solutions, but also to debate and measure needs – both with the defense prime contractors for implementation and integration as well as within the Ministry for specification and deployment.

## A Clear Ethical and Legal Framework to Develop Defense AI

AI raises unique issues when used in defense. Unlike most civilian applications (with a few exceptions, such as health), the use of AI in defense systems requires a particularly rigorous processes to ensure necessary reliability. It also raises questions about responsibility and its division between humans and machines. However, the French defense minister’s speech on 5 April 2019 is very clear about the framework for the development of AI-related technologies:

We will develop artificial intelligence for defense according to three main principles: respect for international law, the maintenance of sufficient human control, and the permanence of command responsibility.<sup>10</sup>

Precautions on ethics have been taken from the start, even if they are state-centric and did not come out of a broader social debate. As far as autonomy is concerned, the minister stated in the same speech that “France refuses to entrust the decision of life or death to a machine, a machine that acts in a completely autonomous manner and is beyond any human control.” It reaffirms the need for human control in all weapon systems to be developed in the future. This position has been codified through Instruction 1618 on the implementation of programs<sup>11</sup> and is also supported by the creation of a ministerial ethics committee on defense issues in 2020. Chaired by Bernard Pêcheur, Honorary President of the Council of State, and vice-chaired by General Henri Bentégeat, former Chief of Staff of the French Armed Forces, the Ethics Committee is made up of 18 members of the Armed Forces as well as external experts. These external experts include a wide range of professions such as lawyers, professors, and researchers. The ethics committee, which has no equivalent in other Western nations, issues advice (e.g., SALA or LAWS – lethal autonomous weapons systems, augmented soldier) while ensuring that the red line – “keep the human element in the loop and do not influence the leader’s decision” – is respected.

---

9 Bômont, “Le cloud défense : défi opérationnel, impératif stratégique et enjeu de souveraineté,” p. 31.

10 Parly, “Statement by the Minister of the Armed Forces on Defense AI in Saclay.”

11 Instruction n°1618/ARM/CAB on armament operations.

According to the reports of this committee, the degree of autonomy of an AI-integrated system can only be determined by considering several inseparable dimensions: the design, the deployment, and the use of weapon systems. This is even more important given the length of the operational life cycle of the equipment, which spans a decade for the most agile systems and several decades for the heaviest equipment. Questions about deployment and doctrine arise more frequently in the development loop due to a goal of accelerating digital procurement programs.

The Ethics Committee further added that the design phase requires in-depth reflection on the future use of the system and its rules of engagement. This allows planners and operators to determine the tasks that will be entrusted to AI and the degree of autonomy it will have to perform. As with vehicles and their level of autonomy, this is not a binary characteristic, but a continuum that needs to be quantified according to progressive levels. The definition and relevance of such a scale in defense has not yet been fully debated, but the need is certain to arise.

# 3 Developing Defense AI

Following Villani's work and the President's speech, France has adopted a national AI research strategy and corresponding funding plan. This strategy is managed by a national coordinator and is part of the management of credits from the "Investment for the Future Program" (PIA) and "France 2030" by the General Secretary for Investment (SGPI). As the Cour des Comptes<sup>12</sup> recalled in April 2023, as part of its evaluation of public policies,<sup>13</sup> the primary objective of France's AI strategy at the time was to avoid falling scientifically behind. As a result, the investments made were initially (2018-2022) concentrated on research and innovation, with a total investment of €1.5bn.

The second phase of the national AI strategy was launched mid-2022, with the aim of accelerating the diffusion of AI in the economy and arranging it so that AI can meet the need to automate ancillary tasks.<sup>14</sup> To achieve this, the acceleration strategy is based on investment to support the deep tech of embedded AI, trusted AI, and frugal AI. The aim is to remove certain scientific hurdles on decentralized or embedded AI. A prominent example is energy-efficient hardware for data processing with AI models at the near-edge with a high-level of trust on high-risk applications.

### 3.3 France's AI Innovation Base

France benefits from a relatively dense academic and research base including institutions such as the National Institute for Research in Digital Science and Technology (INRIA), the French Alternative Energies and Atomic Energy Commission (CEA) or the National Center for Scientific Research (CNRS).<sup>15</sup> Since AI is not considered a discipline, the research component of the French national strategy launched in 2018 has focused on structuring the ecosystem with the creation of AI centers of excellence, through the designation of interdisciplinary AI institutes (3IA), the establishment of individual chairs (43), as well as the identification of centers of excellence outside the 3IA institutes.<sup>16</sup> Cooperation in AI research not only takes place through research projects with public research institutes, but also with universities and engineering schools. For example, the Ecole Polytechnique (Centre Interdisciplinaire de Défense et de Sécurité, CIEDS) launched an R&D center in 2021. With an annual budget of €10M the center shall conduct cutting-edge scientific research in areas of defense interest and connect communities of researchers, students, Ministry of Armed Forces staff, funding agencies, companies, and more.

---

<sup>12</sup> Cour des Comptes is the supreme body for auditing the use of public funds in France.

<sup>13</sup> National artificial intelligence research strategy: a strategy to be structured and sustained.

<sup>14</sup> AI National strategy.

<sup>15</sup> Ezratty, *The Uses of Artificial Intelligence*, p. 606.

<sup>16</sup> *Ibid.*, p. 12.

According to Bpifrance, there are almost 470 French startups specialized in AI. In 2020, the Ministry of Defense reported that around 100 SMEs and AI startups were involved in French MoD projects. The level of fundraising is an indicator of these startups' attractiveness. For example, 223 deep-tech AI startups have raised a cumulative €3.7bn between 2017 and mid-2022 through 391 funding rounds, including €2.3bn in 2021.<sup>17</sup> Despite this, lack of access to this type of investment for French startups, especially those dedicated to AI, is regularly seen as a hurdle, especially at later project stages (late stage and IPO).<sup>18</sup> However, measures have been taken to encourage innovative players to emerge, for example, by creating Definvest<sup>19</sup> and Fonds Innovation Défense (FID).<sup>20</sup> Since its creation, Definvest has made 18 investments, including Kalray and Preligens, while FID has made seven public investments (including Oversight and XXII). In both cases, the objective is to invest alongside private funds.<sup>21</sup>

SMEs specializing in AI involved in defense programs are mostly spinoffs from French research laboratories like CEA or INRIA (Figure 2).<sup>22</sup> The respective network of French AI startups and SMEs is unique in that its members cover all the different technological segments of AI: AI hardware, language processing, data mining systems, voice processing, image processing and data from 3D sensors, right through to autonomy for robotics. The following examples illustrate these capabilities:

- Kalray (founded in 2008) and NanoXplore (2010), for example, specialize in the development of FPGA processors and SoCs
- Oversight (2019) develops software for LIDAR data analysis.
- XXII (2015) offers a software platform for AI video analysis
- Numalis (2015) provides tools and services to help design and validate artificial intelligence systems
- Bloom (2016) develops algorithms for social network investigation
- Delfox (2018) develops a platform to train AI models to train autonomous decision-making systems

---

<sup>17</sup> Ibid, p. 53.

<sup>18</sup> "Web conference on funding and startup development in defense sector." The question of exit is therefore crucial for AI French start-ups. As a reminder, there are three possible options: (1) Acquisition by a large industrial group; (2) Entry into the capital of private equity and specialized investment funds; (3) Initial public offering. While the first option has often been possible, there are few examples of IPOs or French/European capital positioned to finance the final stages of start-ups. This is an obstacle to the development of the industrial ecosystem. This question of exit is all the truer and more problematic for companies positioned in technologies that are considered critical to national security. Multiple rounds of financing can be a double-edged sword. On the one hand, it's an indicator of a startup's attractiveness (and therefore the market-access potential of its solutions and/or innovations) and the possibility of not missing the "time-to-market." But it can also be synonymous with a loss of control (dissolution of capital) and a reorientation of the company's strategy.

<sup>19</sup> With €100M provided by the French Ministry of the Armed Forces, Definvest aims to acquire equity stakes in strategic DTIB (Defense Technological and Industrial Base) SMEs, alongside financial and industrial investors, to enable them to develop independently.

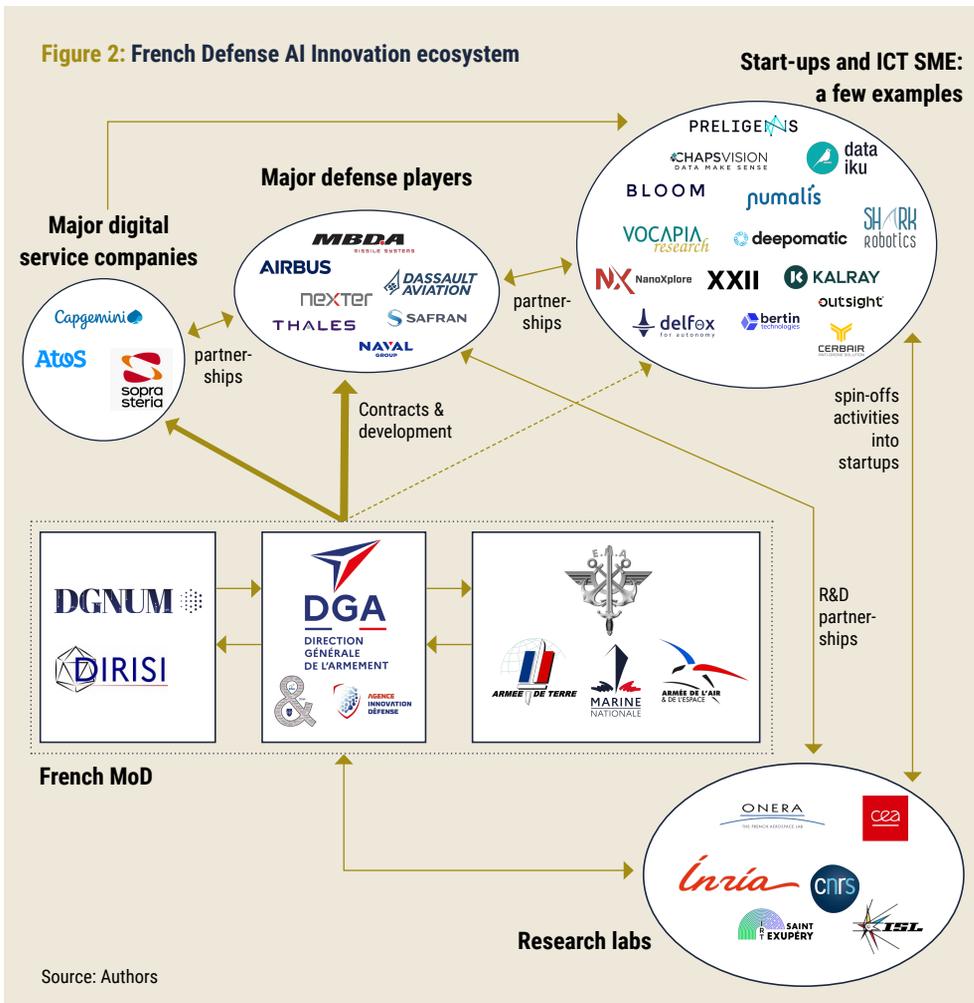
<sup>20</sup> The FID is endowed with €200M. Its aim is to continue the Ministry of the Armed Forces' drive to develop and support of innovation. It is dedicated to the development of dual and cross-disciplinary technologies (outside the traditional DITB players). The fund can invest a maximum of 30% and €20M per company.

<sup>21</sup> Montaufray-Bureau, "The French Ministry of Defense, via Bpifrance, invests in strategic SMEs in Western France."

<sup>22</sup> Parly, "Statement by the Minister of the Armed Forces on Defense AI in Creil."

- Shark Robotics (2016) has rapidly become a key player in the French robotics sector and a benchmark internationally, developing software, hardware and batteries.
- Chapsvision (2019) has established itself as a consolidator in the sector through a highly ambitious external growth policy (more than a dozen company acquisitions in 4 years).

In addition, SME's established in the early 2000s are noteworthy as well. Among them there are, for example, Vocapia Research, a provider of speech-to-text software, and Probayes, specialized in R&D and custom AI engineering. These defense and non-defense SMEs are integrated into the French DTIB ecosystem, either as partners of French prime contractors or as direct suppliers to the French MoD.



### 3.4 Adaptation of France's Traditional Defense Players

The reconfiguration of the IT value chain resulting from digital technological developments is leading digital players (majors, software publishers, digital services companies) to capture an increasing share of the added value generated by companies operating in so-called "traditional" business sectors. Defense is no exception as several civilian and specialized digital players are determined to penetrate the defense market (Table 1). Atos and Sopra-Steria, for example, are involved to varying degrees in the French Ministry of Defense's ARTEMIS.IA program. In 2022, Preligens, created in 2016, had been awarded a 7-year (premium) framework contract by the DGA worth €240M for data processing solutions tailored to defense requirements.<sup>23</sup>

In response, traditional defense prime contractors<sup>24</sup> have adapted their strategies to consider the changes brought on by digital technologies (cyber, cloud computing, AI, etc.). Indeed, the weapon programs for which they are prime contractors are increasingly integrating digital capabilities. Most of these companies' digital transformation plans, which date back to the mid-2010s, include action plans or roadmaps for AI and data governance. However, these specific actions appear to be more recent and coincide with national strategies.

While the strategy of external growth seems to have been favored by defense actors with the first wave of digital technologies related to cybersecurity, current approaches emphasize partnerships and initiatives related to open innovation.<sup>25</sup> To implement a partnership policy, almost all prime contractors have developed corporate venture-type structures or increased their presence within specialized incubators and accelerators. However, there are subtle differences between the different strategies applied by incumbent defense companies:

- Thales is developing its partnership approach with specialized private sector players (start-ups and young SMEs) to ensure long-term collaboration (i.e., move from a prime contractor-subcontractor relationship to a partner relationship). The group has a presence in France at Station F (Cyber) and in Montreal through the Centech incubator (AI). Thales seems to make less use of its corporate venture arm, which is mainly used for strategic actions.
- Airbus Defense & Space has also adopted this approach and has diversified its support mechanisms for its partners, focusing on acquisitions (simplified procedures for subcontractors such as start-ups and SMEs), open innovation

---

<sup>23</sup> "DGA orders data processing solutions tailored to defense needs from Preligens."

<sup>24</sup> Thales, Airbus, Dassault Aviation, Naval Group, Nexter a KNDS Company, MBDA, Safran Group.

<sup>25</sup> Martin, "Defense groups and digital technologies," p. 19.

(more challenges) and its Airbus Group Development structure (support for actors around the Group's various industrial sites).

- Safran Group also launched its corporate venture capital fund in 2015, which has not only allowed it to invest in numerous start-ups in the sector (Outsight, Kalray, for example), but has also structured itself internally to manage and develop its big data activities (creation of Safran Analytics). In January 2021, Safran Group created a new department in charge of driving the Group's digital transformation.
- The situation is different for Dassault Aviation. The company benefits from the positioning of Dassault Systèmes (same shareholder, GIMD), France's leading software publisher (2022 revenue €5.67bn), whose offering is based on the 3D experience platform (modeling-simulation) and, more recently, on the development of a trusted cloud offering (Outscale).

Finally, France's "pure defense players" MBDA, Nexter (KNDS Company) and Naval Group lack synergies stemming from comparable civilian activities. They also seem to suffer from different issues related to data management – such as data access or data storage –, which could be detrimental to their defense AI ambitions. As a result, they might interpret defense AI as a niche task only. However, different specialization strategies are taking place:

- In 2017, for example, the European missile maker MBDA adapted its innovation structure by setting up a "Tech Watch" service to provide technology monitoring. What's more, in 2019, MBDA was selected as a sponsor (along with Thales) in the AI challenge of the Future Investment Program (PIA). In terms of AI, the Group seems to be focusing its approach on topics related to target tracking and identification, especially after its strategic partnership and its acquisition of Kalray. Decision support also seems to be another niche in which MBDA is investing. In February 2020, the Group acquired a stake in Numalis, a start-up specializing in the formal validation of AI-based applications. The Group has also collaborated with Probayes on the HUMAT research program.<sup>26</sup>
- Like other pure defense players, Naval Group opened its innovation structure and system in 2015 with the creation of its disruptive innovation accelerator, the Naval Group Innovation Booster. Like MBDA or Nexter (KNDS Company), Naval Group seems to be positioning itself around very specific AI technologies. Indeed, the group's priorities in the digital field are to strengthen technologies related to digital twins. Other research topics (whether related to the digital twin or not) seem to be predictive maintenance, cybersecurity, and the strengthening of on-board systems (AUV, USV, etc.).

---

<sup>26</sup> Scott, "HUMAT study looks to improve human/machine interface."

- Finally, Nexter (KNDS company) has also reviewed its digital transformation strategy with the creation of a digital innovation and transformation department in June 2018.<sup>27</sup> Within this framework, predictive maintenance, local and global navigation without GPS, and decision support seem to be priority development areas for the group. Issues related to empowerment seem to be a priority for the Nexter Group. As Bruno Ricaud (appointed AI roadmap leader in April 2021) and Cécile Jourdas (Nexter Group artificial intelligence engineer) remind, “in the land military field, autonomous mobility does not yet use artificial intelligence, but traditional robotics methods.”<sup>28</sup> In the field of AI, Nexter’s teams are mainly working on topics related to human-machine collaboration, the validation and certification of neural network algorithms, and the embedding of computing capabilities.<sup>29</sup>

In addition to adapting their innovation structures, defense groups can also jointly develop an offer that incorporates AI or big data capabilities. This partnership, which is part of a defined industrial and commercial project, can be carried out with major digital players, contributing to the digital transformation of the group and its businesses, or with innovative and specialized players (large groups, mid-caps companies, SME and start-ups), mainly in application segments. Focusing on partnerships with major digital players, for example, the Airbus Group has embarked on a data collection project that will enable it to add new services related to fleet management and predictive maintenance. The result is the new “Skywise” (for civil aircraft platforms) and “Smartforce”<sup>30</sup> (for military aircraft platforms) offerings, both developed in partnership with specialist players such as Palantir and Alten.

In addition, as part of the development of a secure cloud offering for Armed Forces and public institutions, European defense contractors have partnered with key players in the field. Thales, for example, has partnered with Google Cloud to position itself in its national public cloud market.<sup>31</sup> Thales and Microsoft are also partners in the development of a defense cloud solution, “Nexium Defense Cloud.”<sup>32</sup>

---

27 Gain, “Comment Nexter conjugue innovation et transformation digitale depuis un an.”

28 Ricaud/Jourdas, “Nexter: AI & Robotic Systems,” p. 28.

29 Ibid.

30 “Airbus launches SmartForce – services bringing the power of data to military operations.”

31 “Thales and Google Cloud announce a strategic partnership to jointly develop a ‘Trusted Cloud’ in France.”

32 “Thales and Microsoft partner to develop a unique Defense Cloud solution.”

**Table 1: Key Actors of the French Defense Industrial Ecosystem Relevant for Defense AI**

French MoD	R&D entities	Defense industrial base
<p><b>Armed Forces AI coordinators, directorates and services</b></p> <p><b>Digital Directorate (DGNUM)</b></p> <p><b>General Directorate for Armament (DGA)</b></p> <ul style="list-style-type: none"> <li>• Operations Directorate and its management units</li> <li>• Technical Directorate and its centers of expertise</li> <li>• Defense system architecture department</li> <li>• Industrial Affairs and Economic Intelligence Department</li> <li>• Defense Innovation Agency</li> <li>• Defense Artificial Intelligence Coordination Unit</li> </ul> <p><b>Staff from the Armed Forces</b></p> <ul style="list-style-type: none"> <li>• Armed Forces Digital Strategy Division</li> <li>• Armed Forces Capacity Coherence Division</li> </ul> <p><b>French Navy, Army, Air Force</b></p> <ul style="list-style-type: none"> <li>• Program planning Divisions,</li> <li>• Digital and innovation entities</li> <li>• Operational units and centers of expertise for the benefit of MSx</li> </ul> <p><b>Joint Directorate of Infrastructure Networks and Information Systems (DIRISI)</b></p>	<p><b>National Research Agency (ANR)</b></p> <ul style="list-style-type: none"> <li>• 4 chairs funded by the French MOD</li> </ul> <p><b>Atomic energy commission (CEA)</b></p> <ul style="list-style-type: none"> <li>• General partnership agreement (joint action under the EDF)</li> </ul> <p><b>National scientific research center (CNRS)</b></p> <ul style="list-style-type: none"> <li>• Framework agreement signed in Sept 2020 - AI study agreement in the process of being signed</li> </ul> <p><b>French National Institute for Research in Digital Science and Technology (INRIA):</b></p> <ul style="list-style-type: none"> <li>• AI agreement signed in December 2019</li> </ul>	<p><b>Traditional defense prime contractors</b></p> <ul style="list-style-type: none"> <li>• Thales</li> <li>• Airbus</li> <li>• Naval Group</li> <li>• Dassault Aviation</li> <li>• MBDA</li> <li>• Safran</li> <li>• Nexter</li> </ul> <p><b>Specialized industries (defense or non-defense oriented)</b></p> <ul style="list-style-type: none"> <li>• Athea (Thales-Atos JV)</li> <li>• Preligens</li> <li>• Chapsvision</li> <li>• Bloom</li> <li>• Dataiku</li> <li>• Vocapia Research</li> <li>• Deepomatic</li> <li>• Kalray</li> <li>• NanoXplore</li> <li>• Bertin Technologies</li> <li>• Shark Robotics</li> <li>• Outsight</li> <li>• Alteia</li> <li>• XXII</li> <li>• Probayes</li> <li>• Delfox</li> <li>• Numalis</li> <li>• Synapse-defense</li> </ul> <p><b>Digital services companies</b></p> <ul style="list-style-type: none"> <li>• Atos</li> <li>• Capgemini</li> <li>• Sopra-Steria</li> </ul>

Source: Authors

## 3.5 Defense AI R&D Strategy

In general, the French MoD focuses on AI-related R&D activities that are underfunded by the civilian sector or require a defense-specific approach. Consequently, R&D activities on AI focus on

- Handling data produced and collected by specific sensors of the Armed Forces such as infrared imaging, Synthetic Aperture Radar (SAR) imaging, sonar, or hyperspectral sensing
- Using AI for very specific military missions such as intelligence collection/gathering or collaborative combat applications
- Developing algorithms for specific tasks such as data and information fusion, heterogenous and multi-source data processing, or weak signal detection
- Ensuring embedded or operational safety challenges stemming, for example, from operating in unknown, unrolled or even hostile environment

The development of defense AI also aims to ensure trustworthiness. This requires the formalization of a dedicated methodological framework and a technological base that allows collection, storage, processing, and exploitation of the necessary data. On the technical side, the Defense Artificial Intelligence Coordination Unit (CCIAD) has published a guide for the integration of AI in operational defense systems. This provides methodological elements for implementation, specification, and qualification.<sup>33</sup> In addition, an initial technology base has been built up around three main projects:<sup>34</sup> ARTEMIS.IA, POCEAD<sup>35</sup> and DATA360/ECE.<sup>36</sup> However, the architecture to store, collect, process, and operate solutions remains to be defined. Pending the next defense cloud program, ARTEMIS.IA remains the most structured program in this field (see also chapter 3.5).

## 3.6 Priority Application Areas

The development of AI in French defense systems is aimed at solving technical defense challenges (specific sensors, embeddability, frugal learning, explainability) to ensure operational superiority. As with any emerging technology, it brings higher levels of performance to operational systems based on maturity. For example, it is now possible to provide feedback from operational deployments for intelligence

---

<sup>33</sup> Guide for integration of AI into programs, 2021.

<sup>34</sup> We can also add Datamar OPS as part of the Navy's data service center (which now holds 1 peta of storage for its data),

<sup>35</sup> Platform for opening up, centralizing, exposing and analyzing data. Developed with Capgemini, in association with Saagie and OpenDataSoft.

<sup>36</sup> Experimentation platform.

applications, while developments in autonomous robotics still require further development.

The French MoD, through its roadmap, has identified seven main use cases for AI in operations:<sup>37</sup>

- Decision and planning support
- Collaborative combat
- Cybersecurity applications and digital influence
- Logistics and operational readiness,
- Intelligence
- Robotics and autonomy
- AI in support services (administration/health).

In view of developing future AI-enabled defense capabilities, the French MoD also emphasizes the need to cooperate with partners. In this regard France acts upon the belief that AI is a technology field ideally suited for multinational cooperation because of its dual use nature. However, French authorities also perceive defense AI as a critical technology.<sup>38</sup> As a consequence, the French Defense Innovation Agency mainly focuses on collaboration within the European context with partners who have complementary capabilities. This is done in part to compensate for French AI-related shortfalls, or to build critical mass. In this context, Germany and the UK have been identified as suitable partners.<sup>39</sup> Outside of Europe, France is building on its long-standing innovation cooperation with Singapore<sup>40</sup> to extend it to AI work. This was demonstrated by the April 2023 announcement of a technical agreement to create a joint R&D laboratory for AI.<sup>41</sup>

---

37 AI in Support of Defense, pp. 14-20.

38 *Revue stratégique de défense et de sécurité nationale*, 2017.

39 *Ibid.*, p.24

40 The SAFARI (Singapore and France Advanced Research Initiative) agreement provides the framework for cooperation between France and Singapore in the fields of research, science and technology. Created in 1997, over the years it has helped to build a solid, trust-based bilateral relationship between state and industrial partners from both countries involved in cooperative ventures. To date, it has carried out over 70 joint projects, notably in the naval, robotics, biological and chemical fields.

41 "France and Singapore create a joint R&D laboratory in the field of artificial intelligence for defense."

## 3.7 ARTEMIS.IA: Ambition and Reality of Building a Defense AI Ecosystem

To address the massive increase in data, the French MOD decided to structure its efforts around a digital foundation in 2017, designed to harness the potential of massive data processing technologies through AI modules. The decision to launch a project, which then became a major procurement program in 2019, was in line with the French MoD's AI strategy goal to harmonize understanding of the issues at stake.

In 2017, the applications developed by the most innovative AI players in the civilian world were developed on outsourced hosting capacities, which enabled them to benefit from standardized interfaces at competitive costs. However, dependence on a private cloud was not an option for activities involving national security. ARTEMIS.IA therefore emerged in a context where there was a strategic need to build a sovereign solution to exploit the mass of operational data from various sensors while facilitating closer ties with the civilian digital ecosystem.

The original ambition of ARTEMIS.IA was to provide shared services for the French MOD's massive data processing applications. This was based on the observation that a single industrial player is unable to meet all user requirements in every context. The technical foundation on which the French MOD's data is hosted has specific features not found in the civilian sector. This includes the need to manage data with different levels of classification. This leads to specific restrictions and multiple security constraints as well as the need to distribute data via networks of varying types, sometimes on embedded platforms.

Alongside this technical ambition, the need to build an ecosystem of applications capable of massive processing around a digital base has raised the need to adjust procurement mechanisms. The innovation partnership, a new feature of the French Public Procurement Code, has made it possible since 2016 to resolve several issues, such as ensuring competitive bidding by contracting the same service to two different manufacturers. It also enables transferring intellectual property from a feasibility contract to a preliminary design and definition contract.<sup>42</sup> This partnership makes it possible to introduce progressive competitive bidding from the exploration phase through to production, culminating in the construction of a market-standard platform. This platform is open to a plurality of business application suppliers and contains a separation of responsibilities: State operator; industrial

---

<sup>42</sup> Article R2172-20 on innovation partnerships – Public Procurement Code.

players developing software bricks; users exploiting them. Through this project, the French MOD explores new ways to engage with startups.

ARTEMIS.IA is divided in three program phases:

- *Phase 1, launched in 2017:* Three players competing in parallel, under the aegis of an innovative partnership framework agreement, to define the foundations of the system and carry out the first proofs of concept.
- *Phase 2, launched in 2019:* ARTEMIS.IA became a program of record. The government selected the ATHEA solution (joint venture between Thales and Atos), a synthesis of the solutions proposed by Thales and Atos in terms of data management, ontology processing and human-machine interface for visualizing the results of data fusion.
- *Phase 3, launched in 2022:* Opening to a diversity of suppliers, including the ecosystem of French AI startups. This has revealed new challenges of integrating innovations of startups into ARTEMIS.IA.

The original design of the program was intended to identify the best proposal among the competitors. However, this objective was not accomplished, as competitors who were unable to win successive phases were eventually able to reposition themselves as subcontractors (despite a ban on co-contracting, and a ban on keeping more than one player after phase 2, circumvented by the creation of the Athea joint venture). Given the criticism of the program, both in terms of ARTEMIS.IA's operational contribution and the relevance of the technical proposal put forward by Atos and Thales, the integration of AI into weapons programs may be subjected to particular attention. This could include more political pressure to be stricter about the competitive nature of such tenders.

As the role of data supervisor is assigned to the DGNUM and not to ARTEMIS.IA, the connections to sensor data (e.g., CSO satellites), the platform for sharing operational data, and the dedicated instances for algorithm training and agile experimentation have not yet been established. This decoupling means that the program has yet to mature. As a result, it does not yet offer a state-of-the-art software platform with genuine integration of innovative building blocks from the civilian ecosystem.

The integration of startups into the ARTEMIS.IA program therefore remains complex: although these startups were invited to take part in phase 1, none of them had the capabilities or the capacity to provide an answer to whole challenge. However, each did have technology that could address parts of the problem. Contacted again four years later, these startups highlighted the difficulty in aligning timeframes between defense programs, the decision-making cycles of major

industry players, the life cycles of start-ups and the ability of the administration to keep up.

It takes a long time for buyers to build up their AI skills, and this has revealed differing levels of maturity among the target users of the first use cases. These are not always aligned with the technological priorities initially defined. For example, French military intelligence services are keen to integrate AI, notably because it can deliver concrete operational gains through technologies that are combat-proven. By contrast, other AI developments – such as detection, reconnaissance, and identification of armored vehicles – have not yet reached full maturity and involve ethical aspects that remain to be solved.

Although it was mainly treated as a technical issue, ARTEMIS.IA also revealed broader organizational challenges. One big issue encompassed the need by the defense procurement agency to reach out to players in all AI-related programs, from the Armed Forces, directorates, and services to industry, and to agree on a roadmap. As a result, ARTEMIS.IA was transformed into a “platform” project, even though it was originally intended as a “profound transformation in the use of data” project, risking selling technology without reflecting on its uses.

# 4 Organizing Defense AI

## 4.1 Defense AI Governance

In 2019, the French MoD created the Defense Artificial Intelligence Coordination Unit (CCIAD) to facilitate the implementation of AI and coordinate the actions of the French MoD. At the time of its creation, the goal was to recruit 200 AI experts and specialists by 2023.<sup>43</sup> Housed within the Defense Innovation Agency (AID), CCIAD's mission is to coordinate the defense AI community, raise awareness of the operational value of AI, and bring together the various stakeholders to communicate on relevant initiatives that can lead to the integration of AI into programs. CCIAD created an ecosystem around two functions:

- AI coordinators in the Armed Forces, directorates, and services, are in charge of cross-functional actions that may affect AI (e.g., those in charge of actions related to ethics or the legal framework), and those in charge of thematic groups related to AI (C4ISR, air, sea, support/health, etc.).
- Project and action managers integrating an AI solution. On the DGA side, this involves AI function architects, AI experts for an armament operation with an AI module or for any upstream study related to AI; on the Armed Forces side, this involves, directorates, services, officers in charge of AI experiments.

However, these coordination functions do not include "data" governance, which is still handled by the MoD's Digital Directorate (DGNUM) as ministerial data administrator.

## 4.2 Data Governance and Data Sharing: A Policy Yet to be Confirmed

Since the launch of its digital transformation process in September 2017,<sup>44</sup> the French MoD's digital governance organization has evolved significantly. Thus, DGNUM was created to carry out this transformation. It is responsible for implementing the Ministry's digital policies (and making proposals for their development). Its director is also the minister's data manager. In this way, DGNUM ensures the implementation of the Ministry's data governance, and its policy is then translated into roadmaps and action plans by the Ministry's various bodies.

---

<sup>43</sup> According to the former coordinator of the national AI strategy, Renaud Vedel, they were 120 to 130. Douillet, «IA: 'Il faut en urgence à la France une force de travail pour préparer, comprendre les données et prévenir les limites des machines.»

<sup>44</sup> La transformation numérique des Armées.

According to the French MoD's 2021/2023 data roadmap,<sup>45</sup> one of the main areas of focus is data exploitation. With a greater variety of data than the civilian sector (e.g., sonar, radar, IR, electronic warfare, etc.), the defense sector is characterized by its specific constraints (embedded systems, limited networks, non-cooperative environment, very often unstructured data). As the main AI solutions on the market focus on deep learning technologies (in particular, machine learning), the development of AI systems relies on the ability to use adapted training and test data. This requires, among other things, massive data annotation. To manage and increase the value of the data, the French MoD has decided to act on three levels: strategic to provide a coherent vision of the data; operational to define sharing rules and exchange procedures; and organizational to promote AI culture.

DGNUM is responsible for implementing a data policy that will enable the identification of existing data, its tagging, and the definition of exploitation models. However, this process of data collection produced in the context of French military operations – data that should then be annotated and contextualized to make it available for defense AI developments – still needs to be structured. It raises many questions: who owns the data, how to store it, how to share it?

In the absence of a general data policy that has been modernized, formalized at a strategic level and shared – an action that is nevertheless called for in the latest French MoD Data Roadmap 2021/2023 – various French MoD entities, have set up discussion frameworks to address the issues inherent in data sharing (e.g., access to data recorded on embedded systems, the consequences of which go beyond the operation of these systems and raise maintenance issues, as platforms now depend on “verticalized maintenance contracts”). This was driven primarily by the operational needs of experimentation with industry support.

Moreover, the French MoD's vision of data sharing seems rather restrictive. The Ministry does not want to share the environmental data sets collected by the system because they are considered confidential and can provide information on the use and performance of defense equipment by Armed Forces and, more generally, on activities carried out in theaters of operations. However, the question of the “value” of the data may be overlooked. It seems that the annotation of the data by an expert in the field is of greater value for the use of AI algorithms than raw data. There are still ways to overcome the sensitivity of operational data, such as anonymizing data by design or creating synthetic data from a data model. Experiments are underway, but the approach is still case-by-case.

---

<sup>45</sup> “Feuille de route de la donnée 2021/2023.”

In addition, different means of accessing data have not yet been clearly debated. This is a problem as different perspectives may collide:

- On the one hand, there is the zero-trust vision developed in the United States by the Chief Digital and Artificial Intelligence Officer (CDAO).<sup>46</sup> This concept assumes that data can only be accessed on the basis of minimal privileges (individual access, need-to-know, etc.) and is therefore based on a restrictive approach (significant compartmentalization of data sources and databases, following a defense-in-depth model as promoted by National Agency for Information Systems Security (ANSSI) in France). In the defense context, with a relationship that is mainly multi-stakeholder (prime contractor, customer(s), subcontractor(s), etc.), this model, based on strict rights management, seems to be the most compatible with confidentiality and data protection requirements. Nonetheless it may have some drawbacks such as the difficulty in configuring multiple logical barriers or over-reliance on this type of solution in the case of an all-in-one model.
- On the other hand, data sharing in an open or semi-open architecture, would be intended to facilitate the use of customer data to improve performance. However, it must be based on the establishment of a trusted industry player, who implements the sharing system according to defined legal and data protection requirements. Additionally, this trusted industry player would need to remain (semi-) open to other solutions, to prevent the risk of vendor lock-in.

---

<sup>46</sup> Kahn, Risky Incrementalism. Defense AI in the United States, p. 25.

# 5 Funding Defense AI

By 2022, the budget for defense innovation increased by around 20% to €1bn. In 2023, this will rise to €1.2bn, intended to enable the Armed Forces to adequately address new fields of conflict (space, seabed, information, cyber) by 2030.

With a target of €100M spent per year on defense AI, upstream studies currently account for almost 30%, the ARTEMIS.IA program for 30% (with a gradual rise to €30M per year), other programs for around 30% (SCAF, Rafale). The remaining 10% are devoted to capturing innovation from the civilian sector via the RAPID<sup>47</sup> grants and the innovation acceleration projects of the Defense Innovation Agency. Investments are mainly focused on use cases considered currently more mature, such as detection, recognition, and identification. AI brings significant added value here, overcoming challenges in terms of the frugality of AI models and state-of-the-art computing.

Spending on artificial intelligence is therefore mainly associated with programmatic roadmaps, decided over a long period of time, leaving very little room for capturing open innovation. The low level of investment to attract military applications of civilian AI innovations therefore complicates the integration of these technologies for the Armed Forces.

**Table 2: Non-Exhaustive List of Major Impact Programs Incorporating AI**

Joint	Land	Marine	Air and Space
<ul style="list-style-type: none"> <li>• SIGINT (DRI: Detection, Recognition, Identification)</li> <li>• Cyber (anomaly detection, deep fakes)</li> <li>• SIA (decision support, planning)</li> <li>• ARTEMIS.IA (maintenance, intelligence, healthcare)</li> </ul>	<ul style="list-style-type: none"> <li>• SCORPION (collaborative combat, DRI)</li> <li>• Eventually MGCS (autonomous robotics)</li> </ul>	<ul style="list-style-type: none"> <li>• SLAMF (DRI)</li> <li>• SHOF (cooperative naval watch)</li> <li>• FDI (DRI)</li> </ul>	<ul style="list-style-type: none"> <li>• FCAS (cooperation remote carriers)</li> <li>• RAFALE (predictive maintenance)</li> <li>• IRIS (DRI)</li> <li>• CELESTE (DRI)</li> <li>• SCCOA (abnormal trajectory detection)</li> <li>• ARES (analysis of spatial object trajectories)</li> </ul>

Source: Authors

<sup>47</sup> RAPID : dual innovation support scheme.

As most programs (Table 2 ) are primarily oriented towards hardware development (as opposed to software), there are several challenges to integrate AI:

- The programs leave little room for increments once they have been launched. Exceptions occur primarily when the industrial company which serves as program and system owner, is ready to commit to performance levels (e.g., purchase orders through MALICIA contracts).<sup>48</sup>
- Most of the funding is earmarked for R&D and the corresponding production at the end of these contracts. Potential scale-up is rarely envisioned. The *Comité de gouvernance du passage à l'échelle* (or Scale-Up Governance Committee) set up by the Defense Innovation Agency is intended to address this issue for all emerging technologies, but with a still limited budget and a restricted number of projects.<sup>49</sup>
- ARTEMIS.IA, the only program to have opened its design phase to an ecosystem of innovative AI players from the civilian sector. It has a budget of €13M to finance the integration of state-of-the-art AI bricks, i.e., barely 13% of the annual defense AI spending.

---

<sup>48</sup> Agile software maturation for the integration of Artificial Intelligence Components.

<sup>49</sup> Briant, "Open Innovation in Defense: Passing Fad or New Philosophy?," p. 11.

# 6 Fielding and Operating Defense AI

## 6.1 A Wide Range of Initiatives

The aim of preparing the Armed Forces for the AI revolution is to help them make the appropriate organizational changes to achieve superior operational efficiency. Initiatives aimed at bringing defense AI to the battlefield take various forms:

### ■ Operational Data Management

In 2020, the French Navy set up a Marine Data Service Center within the Naval Programs Expertise Center (CEPN),<sup>50</sup> with the aim of building up databases annotated and contextualized by sailors. The idea was to make them available to entities inside or outside the French MoD and explore the use of AI to provide decision support tools and use cases exploiting massive data (e.g., electronic warfare, tactical situation replays and sharing, operational readiness, etc.).

### ■ Maintenance, Repair and Overhaul (MRO)

In the French Air Force, the Directorate of Aeornautical Maintenance (DMAé) is leading the strategy to verticalize maintenance contracts. A prime example is the RAVEL program, which groups most of the support activities for the Rafale airframe and associated equipment (excluding the engine). To this end, Dassault Aviation draws on its experience in the civilian sector and uses the same digital tools to carry out all its “support big data” activities.<sup>51</sup> As part of its military support activities, the French aerospace group benefits from sovereign solutions developed by Dassault Systèmes around the civilian 3D Experience platform,<sup>52</sup> an evolution of Catia CAD (having benefited from the acquisition of new technological capabilities, particularly in data mining<sup>53</sup> and *cloud* infrastructures).<sup>54</sup> With the help of these technical tools and a new form of contract, the RAVEL contract has enabled the Armed Forces’ data to be more visible and therefore taken into account.<sup>55</sup>

Maintenance contracts are also designed to address the problem of heterogeneous information systems and the difficulty of communicating between them.

---

50 The CEPN, the Navy’s reference for technical-operational expertise, has been assigned digital service missions by the latest instruction dated 1 August 2022. The Naval Data Service Center (CSD-M) is integrated into the CEPN with various missions: Retrieve, store, process and restore Navy operational data for entities inside and outside the Ministry of the Armed Forces; produce roofs of concept in the field of artificial intelligence, decision support tools using simulation and operational research techniques, and use cases exploiting massive data; act as the Navy’s data reference for technical architectures, artificial intelligence techniques, data processing and data products; provide technical and methodological oversight in the field of data enhancement, in order to federate work on data enhancement and rationalize the Navy’s efforts. For more, see: “Instruction N° 1070/ARM/EMM/MGM.”

51 Dassault Aviation, *Annual Report*, p. 42.

52 3D Experience is a Big Data platform based on Dassault Systèmes’ 3DExperience software, with cloud connection between the Armed Forces and Dassault, without using any American software.

53 June 2010 acquisition of French company Exalead for €135M.

54 Support for the creation of Outscale in 2010 before its takeover in 2017.

55 Industrial maintenance.

In March 2021, for example, Sopra-Steria was selected as part of the Brasidas program, which aims to set up a new information system for aeronautical operational maintenance. Software development is based on a proven civil aeronautical maintenance software package.<sup>56</sup> Thales, the prime contractor for the SCCOA program, is developing the VASSCO information and operational management system, which “ensures the integrity and rapid sharing of information between all players involved in systems support.”<sup>57</sup>

- **Co-Innovation Projects with Industry**

As discussed below, the Military Intelligence Directorate is using short-loop experimentation to develop the TAIIA solution (Image Processing and Analysis by Artificial Intelligence) with Preligens.

- **Feedback Loops for Concept Development**

Feedback from field experience for the development of doctrine, such as the degree of autonomy of equipment, particularly in the context of denial of action in electromagnetic space supports concept development.

- **Training for Specialists and Experts**

The French Army is currently considering the creation of a program for senior officers specializing in AI, big data, and robotics to create a senior management corps.

By operationalizing defense AI along these lines of efforts, the Armed Forces also learn and understand what works or not. On the positive side, the experiments have shown that it is possible to achieve “common requirements” that can be shared across domains/environments despite existing constraints. In addition, experiments also help establish user groups that are essential to collect feedback from operators that helps shape common roadmaps. On the critical side, connectivity – in addition to the decoupling of data, storage, and computing capacities – is brittle. Therefore, Armed Forces need to think about “data frugality” and reconsider whether to put algorithms on the edge or on common backbones. In addition, sometimes operational contexts limit the amount of available data. In this case synthetic data can help to train algorithms. This prompts the need to rethink weapon system contracts and data access, so that algorithms can be constantly evolved and re-trained based on all available data. Recent examples of software factories in the French Armed Forces and the Software Acquisition Pathway in the United States show how hardware/software development cycles can be truly decoupled, with very short software development loops between manufacturers and Armed Forces (a few weeks, or even a few days, instead of several years).

---

<sup>56</sup> “Les armées achètent un système d’information pour accroître la disponibilité de leur avion.»

<sup>57</sup> “Thales wins VASSCO contract to support air surveillance systems.”

## 6.2 Development through Experimentation: A New Approach to Deploy AI Solutions

Developing AI solutions for the Armed Forces involves a great deal of experimentation. Because of the need to access data, the agile development approach required for this technology, and since the level of technological maturity still varies from one application to another, use cases need to be explored with the respective users. In what follows, we look at challenges and the TAIIA case to illustrate the approaches of the French Armed Forces.

### Challenges by the Armed Forces' Experimental Labs

Alongside the DGA's technical innovation clusters and the Armed Forces' experimentation centers, the Armed Forces experimental labs play an essential role in accelerating innovation. Despite their differences in terms of size and resources (whether physical or intangible testing grounds, physical or digital modeling capabilities, with or without a specific location), the Ministry's laboratories share the objective of responding to innovation challenges by working on specific projects or problems.

In 2022, to provide the French MoD with the necessary tools for innovation, the DGA set up the Innovation Défense Lab. This lab provides centralized and dedicated support to the Ministry's laboratories, facilitating hackathons, training courses and design thinking sessions. The Agency has also taken steps to federate the "Defense Makers Community." In collaboration with the DGA expertise center on aeronautical techniques (DGA TA), the Agency presented its ambitions in May 2022, followed by a mapping of the French Armed Forces labs. In this context, numerous exchanges have taken place with entities such as FUSCOLAB,<sup>58</sup> Battle Lab Terre,<sup>59</sup> and CEAM<sup>60</sup> confirming the interest of operational staffs and enabling the French MoD to pursue its efforts to structure this community. The current objective is to create a platform for exchanging and sharing best practices in modeling and rapid prototyping. Ideally, this will accelerate innovation within the French MoD.

One of the latest challenges to consider the integration of AI on the battlefield is the CoHoMa challenge. Aimed at innovation related to decision-making, this challenge focused on displacement (e.g., forest, urban area, open country) and concealment as well as connectivity. Launched in 2021 (and renewed in 2023) by

---

58 FUSCOLAB: Innovation Laboratory of the Marine Fusiliers and Marine Commandos Force.

59 Battle Lab Terre: experimentation lab of Land Forces.

60 CEAM : Air Force Expertise Center.

the Battle Lab Terre, the challenge of cooperation between man and machine aims to unite players in robotics through mixed teams from industry, startups, research labs, and engineering schools around a collaborative challenge. Each challenge envisages a tactical scenario for 2040. Three aspects are of particular relevance: maneuvering and articulating land and air satellites from a master vehicle; crossing terrain compartments and progressing to the final zone; detecting, identifying and deactivating traps to be able to advance while informing the command post.

## Experiments Conducted by Operational Units: The TAIIA Case

The TAIIA project (“Traitement et Analyse d’Images par Intelligence Artificielle” or Image Processing and Analysis by Artificial Intelligence) was an experiment hosted by the Directorate of Military Intelligence (DRM) in 2020.<sup>61</sup> It aimed at building a customized tool for the automatic detection of activities on sites of strategic interest (Figure 3). Based on an experimental platform fed by operational images from the new CSO observation satellite constellation, the project was one of the first experiments to industrialize AI in classified environments. These classified environments imply particular constraints for product development such as on-premises deployment within protected military sites, classified test data, restricted user access, and other aspects. To nevertheless deliver high-performance algorithms, Preligens’ models have been trained on commercial data. Preligens has invested heavily in building an “AI Factory” which accelerates moving from development to production. This has the potential to drastically reduce the time it takes to produce algorithms.

Over and above the challenge of making AI operational for intelligence purposes, the specificity of the project lies in the co-construction of the product. The technology not only helps the experts in their search for information and clues in the images, but also enables them to improve their analysis of activity at pre-selected geographical sites. This project has had far-reaching organizational consequences:<sup>62</sup>

- It has profoundly transformed the activities of photo interpreters and intelligence analysts, freeing them from a particularly tedious task (counting objects) to concentrate on higher value tasks, such as detecting unknown activity on sites of interest (e.g., the presence of drones on a platform where they had never been observed) and thus producing usable intelligence.
- This co-construction approach, which responds to a strong operational challenge but entails major organizational changes, mirrors the defense sector’s unique restraints. The software had to work, heavily restricted, within the

---

<sup>61</sup> “Project TAIIA.”

<sup>62</sup> Ceillier, “Une start-up civile dans la défense, les raisons d’un succès.”

Directorate of Military Intelligence infrastructure and premises, with no Internet connection and no remote intervention in the event of a problem. Preligens transformed its solution in iterations, bringing it into line with the necessary software and operational requirements. Moreover, the end-users, intelligence analysts, remain discrete and bound by oath to secrecy, despite the product's co-construction approach. Many subjects cannot be discussed, and the knowledge passed on is often taken out of context or diluted, preventing direct access to sensitive information. Other adaptations to the agile software development method are necessary due to the constraints of confidentiality such as delivery rhythm (every eight weeks for example, rather than in a matter of minutes or hours in the commercial sector) and user involvement (frequent interaction with users – every day at the beginning of the project and later on a weekly basis via user group workshops – is still unusual in this environment).

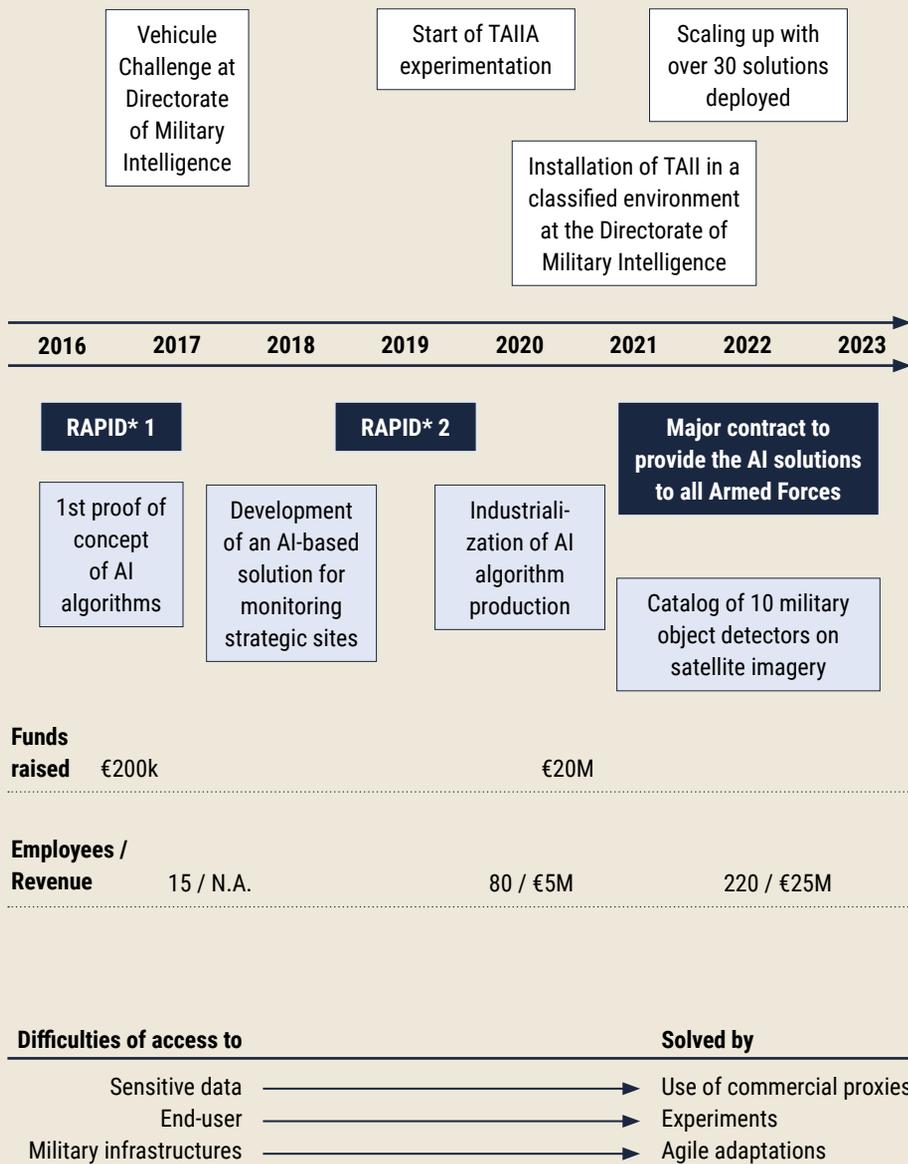
- Finally, despite the operational interest and relevance of the co-innovation approach with AI, this project had to overcome the difficulties associated with scaling up from an R&D budget to industrialization, imposing highly complex contract negotiation phases and specific contractual engineering.
- Initial results have prompted the French Armed Forces to pursue experimentation, with the aim of offering this technological capability to all players in the field of imagery-based intelligence and analysis. After many months of negotiations, the French MoD decided to pursue the TAlIA project, scaling up the solution for operational deployment within the Joint Intelligence Function.<sup>63</sup>

Furthermore, this project also revealed that the historical separation between R&D budgets (P144) and equipment budgets (P146), inherited from the “waterfall” model used for the design and acquire complex hardware systems, was ill-suited for software development in “DevOps”, which requires very short loops between design, development, testing and deployment. The Defense Innovation Agency, via the Scale-Up Governance Committee is addressing this issue to provide budgetary support and leeway for innovation projects that have demonstrated the power to enhance the operational superiority of the French Armed Forces.

---

<sup>63</sup> “France’s General Directorate of Armaments (DGA) contracts with Preligens for data processing solutions to meet its defense needs.”

**Figure 3: The Prelogens Case: The Scale-Up from the TAIIA Experiment<sup>64</sup>**



\*RAPID : R&D project on dual-use technologies funded by the French MOD  
Source: Authors

<sup>64</sup> In 2022, Prelogens signed a 7-year contract worth up to US\$240M with French Defense Ministry. The contract covers the acquisition of software licenses for AI/ML solutions to process and exploit big data.

# 7 Training for Defense AI

One of the last, but nevertheless important barriers to operationalize AI in the Armed Forces remains the human resources challenge. Beyond the subject of AI, the issue of skills in the digital field is crucial. It is essential to have operational staff with a high level of digital expertise. This is currently under considerable pressure due to high demand and limited supply. This situation is reflected in the exponential growth in salaries in the private sector compared to the public sector. Several initiatives have been put in place to meet this challenge:

- The French Interministerial Digital Department (DINUM) has introduced a new approach for the management of its contract staff, based on a “quasi-corps” system. This approach offers several advantages, such as shorter recruitment times, better remuneration for the 56 professions concerned, and a more structured career path. For example, measures are taken to anticipate traineeship and apprenticeship exits to offer positions to qualified candidates. Inspired by the model of the National Agency for Information Systems Security (ANSSI), which employs 80% contract staff, the French Ministry of Defense sees this model as a means of rapid staff renewal, where contract staff come to gain rewarding experience before pursuing their careers elsewhere. This approach fosters diversity of career paths and the enrichment of skills within the administration.
- The use of Digital Service Companies is also widespread, and the French MoD is working to industrialize this collaboration with the private sector. Hybrid service centers have been set up, notably at the Joint Directorate of Infrastructure Networks and Information Systems (DIRISI), to bring together public and private skills to develop satellite links, for example.

Recruiting specialized AI experts is also a challenge for the defense industry. To meet this challenge, major defense companies have created in-house training programs ranging from awareness-raising and dissemination of an AI culture to advanced technical certifications. The co-construction of training programs with engineering schools is also a priority. Projects are launched on interactive simulation using AI, among others at the Air Force Experimentation Center. Finally, we should also mention a partnership initiative between manufacturers (multi-sector),<sup>65</sup> the AI Manifesto. As part of this initiative, which aims to establish a coordinated action plan for the French AI ecosystem, a thematic group (GT) has been set up specifically to address the issues of training and the attractiveness of specialized human resources. The aim is to combine forces, notably by creating a common job repository for the signatory groups of the manifesto and offer synergy in the career paths of young engineers between the different groups (facilitating career mobility between these signatory companies).

---

<sup>65</sup> Thales, Dassault Aviation, Safran, Naval Group. Other signatories include EDF, Total, Valeo, Air Liquide, Renault, Schlumberger, ST, Orange, Michelin, and Saint Gobain.

# 8 Conclusion

Defense AI now seems to be firmly rooted in the French Armed Forces. There is a plethora of initiatives launched in the context of major programs (FCAS, for example), thematic challenges (robotics with COHOMA), or experiments in operational units (TAIIA).

AI governance has also taken shape around the CCIAD at the Defense Innovation Agency. However, considering the requirements of different military services, the Procurement Agency (DGA) and the new entities created as part of the Armed Forces digital transformation (Defense Innovation Agency – AID, the Digital Directorate – DGNUM, Defense Digital Agency – AND), the French MoD's action can appear very fragmented for the defense ecosystem. This is all the truer given that localized, high-impact initiatives have emerged within each military branch at multiple levels, as discussed, for example, with the creation of the Naval Data Service Center (CSD-M).

This profusion of initiatives at various levels and taken by different military branch may illustrate the lack of a centralized data-sharing policy, favoring ad hoc development frameworks. For the time being, the French MoD's approach to data sharing is restrictive. The latest Defense Innovation Agency activity report suggests that this situation is subject to minor changes, with the declared aim of ensure adequate data supply:

Data at the heart of AI-based processing is all the more valuable for its operational nature. The provision of such data must be compensated fairly by the Ministry, such as through the supply of annotated data or the possibility of testing solutions developed by external players.<sup>66</sup>

This type of negotiation generally concerns the sharing of intellectual property related to algorithms developed on the data made available by the MoD. For the time being, however, the respective compensation seems to be negotiated on a case-by-case basis.

In addition, the French MoD's objective is to promote AI in all programs wherever possible and desirable. Indeed, while the first phase consisted of setting a course and providing resources, the French MoD seems to have adopted a new approach, with the widespread dissemination of AI. According to Mickaël Krajecki, head of AI projects at the Defense Artificial Intelligence Coordination Unit (CCIAD), AI is no longer "identified as a particular object."<sup>67</sup> This underlines the French MoD's commitment to a new approach that could be interpreted as a sign of maturity. But it seems that the Ministry's policy remains to be confirmed if it is

---

<sup>66</sup> Defense Innovation Agency Activity report 2022, p. 20.

<sup>67</sup> Vincent/Bezeat, «Défense : les start-ups de l'intelligence artificielle tentent d'investir le champ de bataille.»

to fully disseminate trusted AI solutions. Indeed, if the ministerial policy of data sharing remains restrictive, then this will force the MoD to continue to rely on the recruitment of scarce skilled labor. Moreover, experiments conducted so far have identified major roadblocks such as the need to develop adequate digital infrastructure including clouds, access to users, and adjusting budgetary and contractual mechanisms to the reality of agile software development. The updated defense AI strategy, which could be published by the end of 2023 or early 2024, will need to take these elements into account to meet the challenges of developing trusted AI techniques and solutions.

The strategy update will also need to reflect upon the fact that – despite the will to integrate defense AI into military operations – large-scale implementation has yet to take place. To achieve this, AI governance needs to be strengthened and strategic investments made to develop programs that can catalyze many successful initiatives in different areas of AI. There are still several open items that can help scale AI development, such as:

- Supporting the work of raising awareness of investments in AI within armament programs.
- Increasing financing capacities to scale up AI developments available to major armament programs.
- Increasing the R&T budget of the Defense Innovation Agency's to finance defense applications of emerging civilian technologies, identified and captured in an open innovation process.
- Formalizing a strategic data-sharing policy for the entire French MoD and defining rules of ownership and use to facilitate access for experimentation purposes.
- Decoupling software and hardware development cycles within weapons programs.
- Facilitating agile co-development between the military and manufacturers to move forward on the rapid construction of solutions in response to use cases (possibly drawing inspiration from US Armed Forces' software factories).<sup>68</sup>

---

68 Barrett, "Software Factories for the Military Scale DevSecOps."

# Literature

"Airbus launches SmartForce - services bringing the power of data to military operations", Airbus DS Press release, 16 July 2018, <https://www.airbus.com/en/newsroom/press-releases/2018-07-airbus-launches-smartforce-services-bringing-the-power-of-data-to> (last accessed 30 August 2023).

"DGA orders data processing solutions tailored to defense needs from Preligens", DGA, 12 October 2022, <https://www.defense.gouv.fr/dga/actualites/dga-commande-a-societe-preligens-solutions-traitement-donnees-adaptees-aux-besoins-defense-0> (last accessed 30 August 2023).

"Feuille de route de la donnée 2021/2023," French Ministry of Defense, September 2021, <https://www.data.gouv.fr/fr/datasets/feuilles-de-route-ministerielles-sur-la-politique-de-la-donnee-des-algorithmes-et-des-codes-sources/> (last accessed 30 August 2023).

"France and Singapore create a joint R&D laboratory in the field of artificial intelligence for defense", French MoD Press release, 18 April 2023, <https://www.defense.gouv.fr/aid/actualites/france-singapour-creent-laboratoire-conjoint-rd-domaine-lintelligence-artificielle-defense> (last accessed 30 August 2023).

"France's General Directorate of Armaments (DGA) contracts with Preligens for data processing solutions to meet its defense needs", Preligens press release, 12 October 2022, [https://www.preligens.com/sites/default/files/2022-10/Press\\_Release\\_Preligens\\_DGA.pdf](https://www.preligens.com/sites/default/files/2022-10/Press_Release_Preligens_DGA.pdf) (last accessed 30 August 2023).

"Instruction No 1070/ARM/EMM/MGM relative à l'organisation et au fonctionnement du centre d'expertise des programmes navals," Bulletin Officiel des Armées, no 60, 12 August 2022, <https://www.defense.gouv.fr/sites/default/files/sga/Texte%201%20instruction%20du%201%20aout%202022.pdf> (last accessed 30 August 2023).

"L'intelligence artificielle et le monde de la défense," Direction Générale des entreprises, undated, <https://www.entreprises.gouv.fr/fr/numerique/enjeux/l-intelligence-artificielle-et-monde-de-la-defense> (last accessed 30 August 2023).

"Les armées achètent un système d'information pour accroître la disponibilité de leur avion", La revue du digital, 25 March 2021, <https://www.larevuedudigital.com/les-armees-commandent-un-systeme-dinformation-pour-accroitre-la-disponibilite-de-leurs-avions/> (last accessed date 30 August 2023).

"Project TAIIA", Video, French Ministry of Defense, 2020, <https://www.youtube.com/watch?v=KTqXoYe0uho> (last accessed date 30 August 2023)

"Thales and Google Cloud announce a strategic partnership to jointly develop a 'Trusted Cloud' in France," Thales Group press release, 6 October 2021, [https://www.thalesgroup.com/en/group/investors/press\\_release/thales-and-google-cloud-announce-strategic-partnership-jointly](https://www.thalesgroup.com/en/group/investors/press_release/thales-and-google-cloud-announce-strategic-partnership-jointly) (last accessed 30 August 2023).

"Thales and Microsoft partner to develop a unique Defense Cloud solution", Thales Group press release, 12 June 2018, <https://www.thalesgroup.com/en/worldwide/defence/press-release/thales-and-microsoft-partner-develop-unique-defence-cloud-solution> (last accessed 30 August 2023).

"Thales wins VASSCO contract to support air surveillance systems", Thales, Thales Group press release, 6 January 2022, [https://www.thalesgroup.com/en/worldwide/defence/press\\_release/thales-wins-vassco-contract-support-air-surveillance-systems](https://www.thalesgroup.com/en/worldwide/defence/press_release/thales-wins-vassco-contract-support-air-surveillance-systems) (last accessed date 30 August 2023)

"Web conference on funding and startup development in defense sector," Foundation for Strategic Research, 9 July 2020 <https://www.youtube.com/watch?v=ZKNSIAzZYM> (last accessed 30 August 2023).

AI in Support of Defense. Report of the AI Task Force (Paris: French Ministry of Defense, 2019), <https://www.decideo.fr/attachment/1702015/> (last accessed date 30 August 2023).

AI National strategy: 2nd phase (Paris: Office of the Prime Minister, 2021), [https://minefi.hosting.augure.com/Augure\\_Minefi/r/ContenuEnLigne/Download?id=334FD34F-7844-497E-9551-79EDFF3B2EEF&file-name=1645%20-%20DP%20-%20Strat%C3%A9gie%20Na](https://minefi.hosting.augure.com/Augure_Minefi/r/ContenuEnLigne/Download?id=334FD34F-7844-497E-9551-79EDFF3B2EEF&file-name=1645%20-%20DP%20-%20Strat%C3%A9gie%20Na)

tionale%20pour%201%271A%202%C3%A8me%20phase.pdf (last accessed date 30 August 2023).

Article R2172-20 on innovation partnerships – Public Procurement Code [https://www.legifrance.gouv.fr/codes/section\\_lc/LEGITEXT000037701019/LEGISCTA000037724640/2021-08-26](https://www.legifrance.gouv.fr/codes/section_lc/LEGITEXT000037701019/LEGISCTA000037724640/2021-08-26) (last accessed 30 August 2023).

Barrett, Randy, “Software Factories for the Military Scale DevSecOps,” FedTech, 9 May 2022, <https://fedtechmagazine.com/article/2022/05/software-factories-military-scale-devsecops-perfcon> (last accessed 30 August 2023).

Bômont, Clotilde, “Le cloud défense: défi opérationnel, impératif stratégique et enjeu de souveraineté,” Focus stratégique, n° 107 (Paris: Ifri, 2021), [https://www.ifri.org/sites/default/files/atoms/files/bomont\\_cloud\\_defense\\_2021.pdf](https://www.ifri.org/sites/default/files/atoms/files/bomont_cloud_defense_2021.pdf) (last accessed 30 August 2023).

Briant, Raphaël, “Open Innovation in Defense: Passing Fad or New Philosophy?,” Briefing de l’IFRI (Paris: Ifri, 2022), [https://www.ifri.org/sites/default/files/atoms/files/briant\\_open\\_innovation\\_defense\\_2022.pdf](https://www.ifri.org/sites/default/files/atoms/files/briant_open_innovation_defense_2022.pdf) (last accessed date 30 August 2023).

Ceillier, Tugdual, “Une start-up civile dans la défense, les raisons d’un succès,” La Jaune et la Rouge, November 2021, no 769, pp. 38-41, [https://www.lajauneetlarouge.com/wp-content/uploads/2021/11/Pages-de-JR\\_769-4.pdf](https://www.lajauneetlarouge.com/wp-content/uploads/2021/11/Pages-de-JR_769-4.pdf) (last accessed 30 August 2023).

Dassault Aviation, Annual Report 2022 (Paris: Dassault Aviation, 2022), [https://www.dassault-aviation.com/wp-content/blogs.dir/2/files/2023/06/RA\\_2022\\_VA\\_BD.pdf](https://www.dassault-aviation.com/wp-content/blogs.dir/2/files/2023/06/RA_2022_VA_BD.pdf) (last accessed 30 August 2023).

Defense Innovation Agency, Activity Report 2022 (Paris: Defense Innovation Agency, 2023), <https://www.defense.gouv.fr/sites/default/files/aid/Bilan%20d%27activite%CC%81s%202022.pdf> (last accessed 30 August 2023).

Duillet, Louise, “IA: Il faut en urgence à la France une force de travail pour préparer, comprendre les données et prévenir les limites des machines,” Usbek & Rica, 4 November 2021, <https://usbeketrica.com/fr/article/ia-il-faut-en-urgence-a-la-france-une-force-de-travail-pour-preparer-comprendre-les-donnees-et-prevenir-les-limites-des-machines> (last accessed 30 August 2023).

Ezratty Olivier, The Uses of Artificial Intelligence (Paris: Self-Published, 2021), <https://www.oezratty.net/wordpress/2021/usages-intelligence-artificielle-2021/> (last accessed 30 August 2023)

Gain, Nathan, “Comment Nexter conjugue innovation et transformation digitale depuis un an,” FOB, 6 July 2020, <https://www.forcesoperations.com/comment-nexter-conjugue-innovation-et-transformation-digitale-depuis-un-an/> (last accessed 30 August 2023).

Guide for integration of AI into programs – Reference: DR- Guide S- CAT n°220000. Revised in 2021, <https://www.defense.gouv.fr/aid/actualites/guide-integration-lintelligence-artificielle-ia-programmes-evolue> (last accessed date 30 August 2023).

Instruction n°1618/ARM/CAB on armament operations, <https://www.legifrance.gouv.fr/circulaire/id/44542> (last accessed date 30 August 2023)

Kahn, Lauren A., Risky Incrementalism. Defense AI in the United States. DAIO Study 23/07 (Hamburg: Defense AI Observatory, 2023), [https://defenseai.eu/wp-content/uploads/2023/01/DAIO\\_Study2307.pdf](https://defenseai.eu/wp-content/uploads/2023/01/DAIO_Study2307.pdf) (last accessed 30 August 2023).

La transformation numérique des Armées, Concepts clés (Paris: French Ministry of Defense, 2020), [https://www.defense.gouv.fr/sites/default/files/dgnum/La%20Transformation%20num%C3%A9rique%20du%20minist%C3%A8re%20des%20Arm%C3%A9es\\_concepts\\_cl%C3%A9s.pdf](https://www.defense.gouv.fr/sites/default/files/dgnum/La%20Transformation%20num%C3%A9rique%20du%20minist%C3%A8re%20des%20Arm%C3%A9es_concepts_cl%C3%A9s.pdf) (last accessed 30 August 2023).

Martin, Kévin, Defense groups and digital technologies (Paris: Fondation pour la Recherche Stratégique, 2022), <https://www.frstrategie.org/publications/recherches-et-documents/groupes-defense-technologies-numerique-2022> (last accessed 30 August 2023).

Montaufray-Bureau, Elisabeth, “Le Ministère des Armées, via Bpifrance, investit dans le PME stratégiques à l’Ouest,” Ouest France, 28 April 2023, <https://www.ouest-france.fr/economie/entreprises/entretien-le-ministere-des-armees-via-bpifrance-investit-dans-les-pme-strategiques-a-louest-6177d838-e4fb-11ed-9757-e35473d4e313> (last accessed 30 August 2023).

National artificial intelligence research strategy: a strategy to be structured and sustained (Paris: Cour des Comptes, 2023), <https://www.ccomptes.fr/system/files/2023-04/20230403-strategie-nationale-recherche-intelligence-artificielle.pdf> (last accessed 30 August 2023).

Parly Florence, “Statement by the Minister of the Armed Forces on Defense AI in Saclay,” 5 April 2019, <https://www.vie-publique.fr/discours/271295-florence-parly-5042019-intelligence-artificielle-et-defense> (last accessed 30 August 2023).

Parly, Florence., "Statement by the Minister of the Armed Forces on defense AI in Creil," 10 May 2021, <https://www.vie-publique.fr/discours/279917-florence-parly-10052021-intelligence-artificielle> (last accessed 30 August 2023).

Philippe, Edouard, "Mission letter from the French Prime Minister to Cédric Villani," n°1756/17/SG, 8 September 2017, <https://purpoz.com/media/default/0001/01/81e6a65e224b3de490ecfbd-00b6e40c79bcb3a43.pdf> (last accessed 30 August 2023).

Revue stratégique de défense et de sécurité nationale (Paris: French Ministry of Defense, 2017), [https://www.diplomatie.gouv.fr/IMG/pdf/2017-revue\\_strategique\\_dsn\\_cle4b3beb.pdf](https://www.diplomatie.gouv.fr/IMG/pdf/2017-revue_strategique_dsn_cle4b3beb.pdf) (last accessed 30 August 2023).

Ricaud Bruno and Cécile Jourdas, "Nexter: AI & Robotic Systems", AFA, bulletin n°104, April 2019, p. 28, [https://pfia2021.fr/conferences/apia/actes\\_APIA\\_CH\\_PFIA2021.pdf](https://pfia2021.fr/conferences/apia/actes_APIA_CH_PFIA2021.pdf) (last accessed 30 August 2023).

Scott, Richard, "HUMAT study looks to improve human/machine interface", Janes, 22 November 2019, <https://www.janes.com/defence-news/news-detail/humat-study-looks-to-improve-humanmachine-interface> (last accessed 30 August 2023).

Speech by French President Emmanuel Macron #Aiforhumanity, 29 March 2018, <https://www.elysee.fr/emmanuel-macron/2018/03/29/discours-du-president-de-la-republique-sur-lintelligence-artificielle> (last accessed 30 August 2023).

Villani, Cédric, For a meaningful artificial intelligence: towards a French and European strategy. Rapport de la mission confiée par le Premier Ministre, March 2018, [https://fichiers.acteurspublics.com/redac/pdf/2018/2018-03-28\\_Rapport-Villani.pdf](https://fichiers.acteurspublics.com/redac/pdf/2018/2018-03-28_Rapport-Villani.pdf) (last accessed 30 August 2023).

Vincent, Elise, and Jean Michel Bezat, "Défense : les start-ups de l'intelligence artificielle tentent d'investir le champ de bataille," Le Monde, 27 June 2023, [https://www.lemonde.fr/economie/article/2023/06/27/defense-les-start-up-de-l-intelligence-artificielle-tendent-d-investir-le-champ-de-bataille\\_6179459\\_3234.html](https://www.lemonde.fr/economie/article/2023/06/27/defense-les-start-up-de-l-intelligence-artificielle-tendent-d-investir-le-champ-de-bataille_6179459_3234.html) (last accessed 30 August 2023)



## Defense AI Observatory Studies

- 23|17** Kévin Martin and Lucie Liversain, A Winding Road Before Scaling-Up? Defense AI in France
- 23|16** Sami O. Järvinen, Cautious Data-Driven Evolution. Defence AI in Finland
- 23|15** Inbar Dolinko and Liran Antebi, Embracing the Organized Mess. Defense AI in Israel
- 23|14** Alastair Finlan, A Fertile Soil for AI? Defense AI in Sweden
- 23|13** John Lee, "Overtaking on the Curve?" Defense AI in China
- 23|12** Heiko Borchert, Torben Schütz, and Joseph Verbovzsky, Master and Servant. Defense AI in Germany
- 23|11** Katarzyna Zysk, High Hopes Amid Hard Realities. Defense AI in Russia
- 23|10** Yvonne Hofstetter and Joseph Verbovzsky, How AI Learns the Bundeswehr's "Innere Führung." Value-Based Engineering with IEEE7000™-2021
- 23|09** Robert C Engen, When the Teeth Eat the Tail: A Review of Canada's Defence Artificial Intelligence
- 23|08** Çağlar Kurç, Enabling Technology of Future Warfare. Defense AI in Turkey
- 23|07** Lauren A. Kahn, Risky Incrementalism. Defense AI in the United States
- 22|06** Yvonne Hofstetter, Wie KI Innere Führung lernt. Wertbasierte Technik mit IEEE7000™-2021
- 22|05** Andrea Gilli, Mauro Gilli, and Ivan Zaccagnini, Exploring the Benefits of a New Force Enabler: Defense AI in Italy
- 22|04** Kenneth Payne, Bright Prospects – Big Challenges. Defense AI in the United Kingdom
- 22|03** Heiko Borchert, Christian Brandlhuber, Armin Brandstetter, and Gary S. Schaal, Free Jazz on the Battlefield. How GhostPlay's AI Approach Enhances Air Defense
- 22|02** Peter Layton, Evolution not Revolution. Australia's Defence AI Pathway
- 21|01** Heiko Borchert, Torben Schütz, Joseph Verbovzsky, Beware the Hype. What Military Conflicts in Ukraine, Syria, Libya, and Nagorno-Karabakh (Don't) Tell Us About the Future of War

