

AI and the Future of Defense

How Defense Must Adapt to AI



By

Major Brice Marty and Major Fanny Peluttiero

French War College



Abstract

In August 2020, an artificial intelligence algorithm outperformed a human F-16 pilot in a simulated 5-0 dogfight competition hosted by the Defense Advanced Research Projects Agency (DARPA). The outcome illustrates the capabilities of AI, which surpass those of humans in many areas. Progress made over the last decade in AI, machine learning and deep neural networks has enabled the development of many such systems, and their application to Defense, a process which too often remains decentralized and chaotic, presents both opportunities and challenges that must be addressed carefully. So as not to miss out on this inevitable technological shift, it is imperative to ask what measures need to be implemented today to enable the effective development of AI tomorrow. Primary among such measures is an efficient and effective data capture strategy, while other measures include a careful selection of a few AI related projects, to generate interest among decision-makers, as well as the emergence of a specific human resource policy to attract highly-sought after talent to work for Defense. The paradigm shift initiated by the digitization of society calls for a strategic adaptation of the relationship between civilian companies and Defense regarding the acquisition of digitized equipment (“Buy”) versus its Defense-led development (“Build”). Overall, organizational adaptability geared towards centralizing digital entities appears likely to be the major enabler in striving to meet this ambitious challenge of integrating AI into Defense.

Executive Summary

Why integrate AI into the military?

- AI offers **technical opportunities** to lighten the cognitive load of combatants, as this has become heavier in recent decades (multi-domain combat, an exponential increase in the complexity of the battlefield and weapon systems)
- Our allies and potential competitors are investing massively in AI, it is therefore crucial that French Defense take an interest in it to foster **interoperability** within the framework of a coalition, ensure **operational superiority** in the event of high-intensity conflict, and maintain an **efficient defense apparatus** commensurate with national ambitions.
- AI is a **maturing technology** that is changing our societies, so this is the right time to exploit the power of algorithms and their application to a range of military functions

Why and under which conditions is it ethically viable to use AI on the battlefield?

- Keep **humans in the loop**
- Use AI systems with awareness of their limits and under the conditions for which they were designed
- Breaking the "**black box**" effect to make the results of the machines explainable

AI integration roadmap:

- 1- **Start small, think big** : select a finite and limited number of pilot projects
- 2- No data ➔ No AI : define a specific **data strategy** (collect, capture & refine – governance - cloud) tailored to the selected pilot projects
- 3- Solve Defense's strategic dilemma of whether to "**make**" or "**buy**" (strategic issue or exclusiveness of data = make, otherwise buy)
- 4- Develop armament & a **digital ecosystem** (Start-ups & Industry + digital Giants & Industry)
- 5- Recruit specialized **human resources** to implement, explain and exploit AI
- 6- **Governance** & organizational adaptation
- 7- Develop a **digital culture**

Summary

- Executive Summary** 1
- I. Introduction** 5
- II. Will AI be the next battlefield game-changer?** 5
 - A. Why AI represents a major challenge as a systemic and disruptive innovation 6
 - B. Legal and ethical issues..... 6
 - C. Technology and Defense ecosystem readiness for AI integration 7
- III. Minister of Defense roadmap to better integrate AI**..... 8
 - A. First step: develop a targeted data capture strategy..... 8
 - B. New technologies require the development of new partnerships..... 11
 - C. Governance 15
- IV. Conclusion**..... 18
- V. Appendix 1: business model for AI integration within Defense ecosystem** 20
- VI. Appendix 2: press release announcing the contribution of AI in armed operations** .22
- Bibliography** 23

AI and the Future of Defense

How Defense Must Adapt to AI

I. Introduction

In August 2020, the Defense Advanced Research Projects Agency (DARPA) organized the AlphaDogfight competition as part of its Air Combat Evolution (ACE) program, which aims to strengthen the "man-machine" interface in air combat. During the competition, AI algorithms were tested by a threat replicating algorithm and then competed against each other; after this, to determine the best performance, they went up against an experienced F16 pilot on a simulator. All algorithms were subject to the technical limitations of an F16 and its pilot so as not to disadvantage humans. Despite this precaution, Heron System's algorithm still dominated the human pilot during the five single combat situations in which they were engaged. The reason is simple: AI was not limited by "the training and reflexes that are ingrained in a pilot"¹ and the decision loop² was much faster for the automated system, even if only on the order of nanoseconds.

In addition to the tactical and technical feat accomplished, this experiment had the goal of increasing the confidence of the feasibility of using artificial intelligence in combat aircraft³. AI is no longer at the stage of testing performance, but of proving to humans that these systems are trustworthy because they perform better than humans.

From home and work lives to the theatre of war, since the early 2000s AI systems have become more and more powerful and now outperform humans in many areas, such as chess, the game of Go or even mass data processing and medical image recognition. The progress made over the last ten years in machine learning and deep neural networks has enabled the development of these systems, and their application to Defense presents opportunities that must now be considered with the utmost care. The significant investments that China, the United States and Russia are making in AI are objective indicators of the importance given to it today. To maintain operational superiority, it is imperative to study the opportunities offered, the limits linked to military singularity, the means to be equipped and the strategy to achieve all of this.

In spite of the French political will to develop an AI for Defense, implementation is still incomplete because it remains decentralized and chaotic. To prepare for this inevitable future and so as not to miss out on this technological shift, it is imperative to ask what measures need to be put in place today to enable the effective development of AI tomorrow.

The key to the successful integration into Defense equipment relies on meticulous preparation through an immediate implementation of a data capture strategy. The paradigm shift initiated by the digitization of society calls for a strategic adaptation of the relationship between civilian companies and Defense in the context of the acquisition of digitized equipment. An organizational adaptation geared towards centralizing digital entities appears likely to be the major enabler in striving to meet this ambitious challenge.

II. Will AI be the next battlefield game-changer?

¹ Everstine Brian W., "Artificial Intelligence Easily Beats Human Fighter Pilot in DARPA Trial", August 20, 2020, <https://www.airforcemag.com/artificial-intelligence-easily-beats-human-fighter-pilot-in-darpa-trial>.

² Decision loop OODA: Observe Orient Decide Act

³ Everstine Brian W., "Artificial Intelligence Easily Beats Human Fighter Pilot in DARPA Trial", August 20, 2020, <https://www.airforcemag.com/artificial-intelligence-easily-beats-human-fighter-pilot-in-darpa-trial>.

A. Why AI represents a major challenge as a systemic and disruptive innovation

AI constitutes on the one hand a systemic innovation⁴ (SI) because it can be successfully integrated into another system, because it is synergistically coordinated with other innovations in a complete ecosystem. It goes beyond the boundaries of a single organization to modify the society. AI is also a disruptive innovation (DI) because it follows an incremental process of integration. AI initially takes root in simple applications at the bottom of a market and will relentlessly move upmarket⁵. It requires the exploration of new technological attributes and customer segments, prompting firms to dedicate specific business units to the “disruptive innovation job” (Christensen, 1997).

Finally, AI is also considered as a breakthrough technology because it introduces a radically new capability or a drastic performance improvement. It literally means a technology that has broken through some kind of obstacle or barrier, or may indicate a sudden advance. These kinds of technologies are at the heart of radical innovations, which transform or create new markets⁶.

This kind of technology has significant consequences regarding the balance of global power. If we consider the example of engines during the 19th century, the direct consequence of this innovation was the development of tanks and trucks; then, indirectly, of planes, which eventually led to drones. Engines launched a new competition regarding operational superiority and profoundly impacted the military, in particular during WWI. Engine technology transformed the battlefield and the means of waging war by accelerating the speed of decision-making, both tactically and logistically.

These definitions suggest that AI will not only transform military material and process, it will also bring about deep transformations in organizations and mindsets. Defense has to be ready to support rapid, even revolutionary developments in the future due to digital progress in AI in particular; and as a consequence, in edge computing, education, acquisition and development process and partnerships.

As a consequence, it is necessary to consider whether the legal and ethical framework matches with this new and disruptive technology.

B. Legal and ethical issues

Before implementing this kind of technology on the battlefield, it is necessary to study the legal and ethical issues of AI and autonomous systems. C. Anthony Pfaff⁷ analyzes this problem and introduces the notion of a "responsibility gap"⁸ related to the "black box" effect cumulated with the human holistic knowledge and understanding of the world which remains impossible to program. These two phenomena can induce errors in an autonomous system without being able to designate a responsible person based on the law currently in force.

In order to remain in conformity with the laws of war, as well as international humanitarian law, states must, according to Pfaff, develop this notion of responsibility for the use of autonomous and semi-autonomous systems, which could imply the following:

- the need to explain/justify? any decision made, or fact generated, by a machine; this is actually possible by adding a double algorithm in parallel of the calculating algorithm. The double one should follow the operations of the first algorithm to explain the results.
- constantly ensuring the machine is employed in the situation for which it has been designed, technically, tactically and ethically;
- employing these systems only when the level of violence justifies it;

⁵ Christensen, Clayton M.; Bower, Joseph L. (1995), "Disruptive technologies: catching the wave", Harvard Business Review

⁶ Garcia, R. and Calantone, R. (2002), A critical look at technological innovation typology and innovativeness terminology: a literature review. *Journal of Product Innovation Management*, 19: 110-132.

⁷ Research professor for the Military Profession and Ethics at the Strategic Studies Institute of the US Army War College

⁸ Pfaff C.A. (2019) “The Ethics of Acquiring Disruptive Technologies: Artificial Intelligence, Autonomous Weapons, and Decision Support Systems”, *PRISM Singularity* VOL.8 NO.3: 128-146

- "establish[ing] standards for diffusing responsibility⁹";
- regulating the proliferation of these weapons, in particular fully autonomous systems;
- specifying conditions of employment while "preserve[ing] the military identity and address[ing] conditions that give rise to desensitization and other psychological trauma".

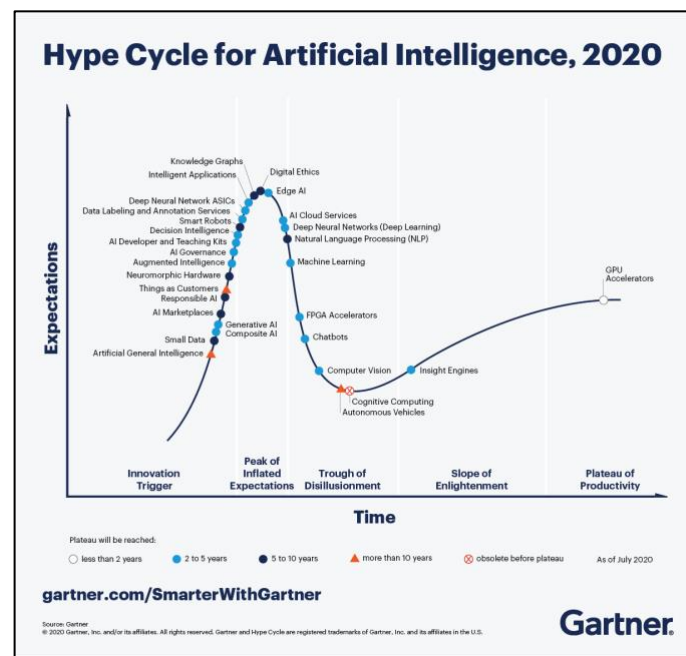
However, before these recommendations actually take effect and the technology is sufficiently mature to be implemented, it is imperative to keep people in the decision-making loop and to educate both operators and leaders. This is particularly true with respect to the decision to open fire and potentially take human lives.

Every user must be aware of the potential errors of autonomous systems, be they related to learning data or a potential security breach, all of which must be put in an operational context where benchmarks can be modified. Like the 1988 incident when the USS Vincennes shot down an Iranian airliner, when the Aegis ground-to-air defense system, fully autonomous but under human supervision throughout its decision-making cycle, identified an Iranian F14, even though the data indicated that it was a civilian aircraft. 290 passengers were killed due to a misunderstanding regarding the system's level of autonomy.

This could have been avoided with a clearer definition of responsibility. This definition should complement international and humanitarian law through consensus. Work on the topic is ongoing and will be completed in the coming years as the level of maturity of these technologies becomes clearer.

C. Technology and Defense ecosystem readiness for AI integration

Each year Gartner offers tools for analyzing emerging technologies related to the economy and investments, including the Hype Cycle. It evaluates each year the relative market promotion, maturity and value of innovation relatively to a technology area. Regarding AI, the Hype Cycle published in 2020 by Gartner shows that the technologies are currently experiencing its "trough disillusionment": after a peak of interest and investment in recent years (2015-2019), some technological promises have been disappointing and led to a decreasing of investment and interest before reaching a certain maturity of use and development.



⁹ Pfaff C.A. (2019) "The Ethics of Acquiring Disruptive Technologies: Artificial Intelligence, Autonomous Weapons, and Decision Support Systems", PRISM Singularity VOL.8 NO.3: 128-146

Today, the results of the R&D carried out specify the opportunities that AI will enable today and in the medium term, free from any technological fantasy, but also the benefits to be gained by organizations. "AI is starting to deliver on its potential and its benefits for businesses are becoming a reality¹⁰".

According to Gartner, the new challenges now lie in human resources, like developers who are the "major force in AI," and in governance, which is a "priority," in particular "on an industrial scale".

As far as Defense is concerned, it is not immune to future challenges, as will be explained below. However, it has already taken into account that AI offers and will offer capabilities that are of interest to armies in their missions as well as in their organic functioning. Through several government Villani report in 2018) and ministerial publications (Artificial Intelligence for Defense in 2019, report of the AI Task Force 2020), France and the French Ministry of Defense have grasped the need for investment in this area to maintain a high level of technology of Defense systems.

At the same time, investments have been made to improve AI's integration via the investments of the Defense Innovation Agency which defined AI as a priority in 2019, the development of investment funds (Definvest, the strategic place) and support for research projects like ASTRID, RAPID, ASTRID maturation. These measures take into account the necessary flexibility and plasticity advocated in strategic documents, but also the need to expand and recast the military innovation ecosystems that are too rigid for the rapidly evolving digital world.

Within this strategic, legal and ethical framework, it still seems necessary to define a concrete and coherent roadmap to enable the integration of AI in military systems of today and tomorrow, starting with the fuel of any artificial intelligence system: data.

III. Minister of Defense roadmap to better integrate AI

A. First step: develop a targeted data capture strategy

Integrating AI within the Defense sector makes sense if it will provide an operational or tactical advantage, even if it is limited to a specific domain. Indeed, introducing an innovation for the sole purpose of possessing a state-of-the-art technology would not make sense. Artificial intelligence should only be integrated into military systems if the technology is mature enough and it provides a real advantage over previous technologies. Prior to any AI integration in the military, Defense has to define a targeted data capture strategy based on realistic and specific applications to enhance operational superiority.

1. AI at the service of operational superiority: define few pilot projects

The art of war cannot be summarized as a mathematical table that would ensure victory. However, respect for the fundamental principles is essential to optimize the chances of success. The top economic powers are pursuing a continuous quest to transform and adapt their military capabilities to fit operational realities. Furthermore, according to Clausewitz¹¹, building success on the battlefield relies on the art of maneuvering troops and arms to maximize the effect on the opponent. AI could confer a real advantage in three specific domains so as to acquire operational superiority in combat:

- The mass that combines technological superiority and volume of force: a good articulation of these two factors gives the opportunity to gain the upper hand over an adversary;
- Operational expertise: the art of combining the available arms effects against an enemy or on the environment adequately within the context;
- Information mastery represents a dual challenge in modern warfare: assessing the situation and acting on the adversary's will to fight.

¹⁰ Goasduff Laurence, "2 Megatrends dominate the Hype Cycle for Artificial Intelligence, 2020", September 28, 2020, <https://www.gartner.com/smarterwithgartner/2-megatrends-dominate-the-gartner-hype-cycle-for-artificial-intelligence-2020/>

¹¹ Clausewitz C.V (1832) "Principles of War", the Military Service Publishing Company, translated and edited by Hans W. Gatzke in 1942

While there is consensus identifying AI as a technology which will become unavoidable in the future, governments, businesses and the whole of civil society are forced to identify the issues at stake in this societal transformation and all the implications this has for living things.

Beyond the predictions of the advent of an AI that would surpass the human being in every area, many applications are so challenging that they are able to replace or even outperform any human being in specific tasks requiring human intelligence: on January 15, 2018, Microsoft announced that its algorithm had succeeded in beating a human being in a reading test¹². Microsoft's AI obtained a score of 82.65 against 82.30 for the human.

As a result, many military systems could already benefit from the computing power of deep learning or machine learning algorithms with the exclusive aim to assist human cognition in more impactful decision making, while retaining effective human control in all circumstances. Defense must invest, starting today, in systems that will exploit the power of AI algorithms in three key areas: the construction of Situational Awareness, the control of the life cycle of weaponry and the automation of certain military systems.

As a prerequisite for any use of AI algorithms in weapon systems, Defense has to develop a data capture strategy for each of these three areas of interest. However, any dispersal of attention and means to collect data in all directions towards the creation of a “data lake”¹³ would be counterproductive. The data capture strategy should be limited to well-identified applications, considered as pilot-projects, designed to improve operational efficiency. These applications are not universal and remain interdependent on the fundamental characteristics of each country. France, for example, which has a medium-sized Defense apparatus with strong operational experience relying on high technology, should invest in technologies which profit from these strengths and mitigate their weaknesses.

2. Which AI integrated applications meet these three requirements?

Regarding AI and mass, real-time image analysis applications would significantly increase the technological capabilities of the weapon systems currently in service. Indeed, the operational superiority of modern armies relies first and foremost on a quest for identifying and clarifying the "Situation Awareness"¹⁴ to dispel the fog of war. These tools for optimizing DRI (Detection, Reconnaissance and Identification) capabilities would concomitantly help speed up the operational tempo by relying on the algorithm's ability to instantly process information and present the best options, all while minimizing the risk of collateral damage, which can have dramatic strategic consequences.

In addition, AI could optimize the readiness rate and improve logistics. While robotics associated with General Artificial Intelligence (GAI) would finally serve to reconcile the search for technological superiority with the volume of forces, technological discoveries remain insufficiently mature to invest immediately and massively in these autonomous systems. However, a medium-size army in terms of volume, such as that of France, could already benefit from the capabilities of algorithms to improve its technical operational capability. The introduction of AI in maintenance software and, more generally, in supply chains would help minimize equipment downtime and contribute to increasing the number of forces able to oppose an adversary.

AI algorithms could also enhance operational expertise while improving maneuvers and decision-making. Training centers are already equipped with digital systems for after-action analysis. These

¹² The Stanford Answering Dataset (SQuAD) is a reference reading test which consists in asking more than 100,000 questions from 500 Wikipedia articles.

¹³ A data lake is a centralized repository that allows you to store all your structured and unstructured data at any scale. You can store your data as-is, without having to first structure the data, and run different types of analytics—from dashboards and visualizations to big data processing, real-time analytics, and machine learning to guide better decisions. (AMAZON AWS)

¹⁴ Endsley M.R. (2000) “Situation Awareness analysis and measurement”, CRC Press

simulated combats opposing the trained forces to a real opposition force, in an ultra-realistic environment, have been digitized for nearly ten years. The analysis of this accumulated data by an AI-based system could open up new perspectives for decision-making tools at levels 4 and 5, and could even be used in support of after-action analyses. These tools would provide dual benefits: one based on the reinforcement of the knowledge acquired at each rotation; and another as a decision-making tool for future combat.

Finally, AI could optimize that information mastery and management that is essential to perceiving, interpreting and exchanging large amounts of data in order to develop and maintain the situational awareness requisite for successful decision-making. Information sources have significantly multiplied of late - satellites, UAVs, sensors on all types of vehicles - to the point where human analysts are overwhelmed with information. It seems obvious that the computational capabilities of algorithms to analyze huge masses of data, to identify salient facts, or even make connections imperceptible to human cognitive abilities would be a tool conferring significant operational advantage at every level regarding the building of situation awareness.

3. The data strategy roadmap is based on 4 interdependent steps

The approach to data strategy (collection, storage and exploitation) is essentially aimed at improving human or automated-system decision making, once these are enriched with AI algorithms. This data-centric strategy requires a complete rethinking of the organization and operational processes in order to exploit the full potential of data. The necessary evolution of the Geospatial Intelligence Analysts' job (GEOINT) is a perfect illustration of this dependence on data. Their role is decisive in this perpetual quest to build the best "situation awareness" in current operations: their vocation is to merge all intelligence data (images, human and electromagnetic intelligence) on the same geo-referenced map, yet they are regularly overwhelmed by flows of information. Automatic image processing and machine learning tools, enabling the aggregation of information from various sources (Multi-INT), could provide headquarters with strategic knowledge to acquire information superiority, better and faster than any human analyst could provide.

Step 1: Data collection and storage acquisition

Once the applications where AI could be a significant asset for operational superiority have been identified, Defense needs to establish an efficient data strategy. The process should initially consist of identifying information already acquired by the armed forces, then defining the vectors that will enable the missing data to be collected and fed into the application algorithms, while then acquiring storage and computing resources. Taking the example of satellite images containing a large amount of information used to assess the situation in many areas of the globe, the use of Artificial Intelligence would make it possible to automate a large part of this analysis from just a few pixels. However, it is first necessary to collect a vast reservoir of satellite images and ensure computing capacities able to exploit the power of AI.

Step 2: Algorithms development and curated data¹⁵

The advent of machine learning and deep learning was only made possible with the processing of big data. The complexity of algorithm development, as well as its efficiency, is dependent on the quality of raw data transformation (operationalization). Therefore, the simplicity of coding, as well as the performance of the algorithms, are interdependent regarding data curation, which consists in collecting, organizing and managing a collection of data sets.

Regarding the GEOINT analysis framework, the power of image analysis algorithms could even detect objects that exist in very small numbers among more numerous images. Some applications (such as Preligens), offer solutions for data operationalization that improve the performance of the algorithm

¹⁵ Dave Wales, "what is data curation", February 2020, <https://www.alation.com/blog/what-is-data-curation/>

while minimizing the number of examples needed for training. They reinforce the efficacy of the tool and allow systems to learn from fewer labeled examples.

Step 3: Establishment of data governance

A critical part of the data for Defense strategy is also the establishment of data governance, which in turn depends on the development of a data culture within the organization. Indeed, success will rely on a multi-stakeholder approach that is both civilian and military - data scientists, military experts and industrialists - involved in this project to establish effective data management and sharing procedures where the main objective is to make information usable at the right time, in the right place and by the right person. Data governance is paramount in the example of automated geospatial intelligence analysis. Coordination between civilians and the military is essential, as the relevance of the tools developed by Preligens is based on the aggregation of information from various sources (Multi-INT), such as imagery (ROIM), signals intelligence (ROEM) or open source (ROSO), in order to deliver an analysis that is perfectly adapted to the military requirement.

Step 4: Migration of data

Once the data collection and exploitation strategy has been developed, migration to the cloud remains a critical and sensitive step. This involves ensuring that the extracted data undergoes a series of preparatory actions before it can be uploaded to the target location.

A strategic data migration plan consists of four incremental stages:

- Knowledge of data: Prior to migration, source data must be carefully analyzed and identified;
- Clean-up: correction of errors identified in the first phase;
- Maintenance and protection: data must be monitored because it degrades after a certain time, and the data must be secured, especially if it is strategic;
- Governance: Once the data has been uploaded, it must be streamed via the establishment of procedures and tools that are user-friendly and automated to the fullest possible extent.

4. Building a solid foundation before the advent of global AI

The technology is not yet mature enough to consider an efficient use of fully autonomous systems. Moreover, the performance requirements inherent in the use of this type of military-oriented system add to the complexity of the unstructured battlefield environment.

However, armies can already anticipate the advent of these technologies by collecting the data needed to train future algorithms. For that, they also need AI experts and technicians with the skills and technical know-how to first assess, study and build programs and data strategy, and then lead them to success. Following the example of the automotive industry, which is iteratively improving vehicle automation, Defense must develop scalable weapon systems that offer the opportunity to integrate an automation function at a later date.

Investing in relatively inexpensive, automated UAVs in all three physical environments (land, air and sea) would appear to be a relevant solution. These systems could be used immediately in theaters of operation, supplementing manned vehicles to increase the tactical mass to be deployed against a potential adversary, especially in the case of large-scale conventional operations.

There is also another advantage to having automated UAVs in a high-intensity conflict context: if the networks necessary for AI operation were to be scrambled, armies would still have the capacity to use unmanned weapon systems in degraded mode (traditional UAVs).

B. New technologies require the development of new partnerships

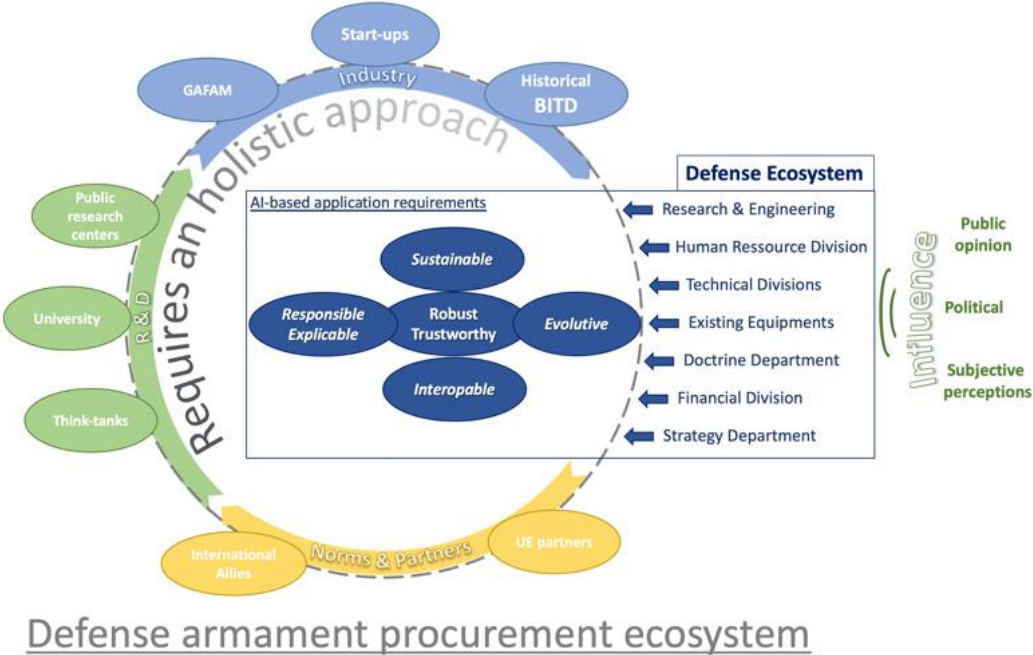
The current armament procurement process is not suitable to the innovation tempo of digital technologies. The MoD's procurement policy aims to meet the needs of armies for the acquisition of systems and services in order to contribute to the operational efficiency of armed forces. The frenetic pace of discoveries in digital technology requires an adaptation of purchasing processes.

The armies, even those of superpowers like the United States and China, are no longer the driving forces behind research in these cutting-edge technologies. Civilian industry has taken the lead regarding their development, transposition and integration upon maturity. This paradigm shift requires armies to reform the acquisition cycle and create a new ecosystem through a multi-stakeholder approach because the traditional Defense industrial base has a hard time adapting to digitization.

1. The strategic dilemma of Defense regarding AI: “build or buy?”

Which digital ecosystem best suits Defense needs?

Beyond the difficulty of identifying cases studies where AI would confer real added value, most major industrial groups, whether Defense or not, are increasingly using technology partnerships to develop tools that integrate high-performance AI. By partnering with AI players, manufacturers rely on technological know-how to develop customized solutions. Reciprocally, AI stakeholders identify this opportunity to sign long-term contracts as a lever for the development of their company.



Artificial Intelligence market overview:

The AI market spans a multitude of sectors and is so vast and intertwined it can hardly be delineated. Unsurprisingly, the main driving forces behind these developments are the big five, as they benefit from a complete digital environment as well as unlimited funds to develop their own AI technologies.

Companies at the top of Gartner's "Magic Quadrant", even if they are sometimes reluctant to interact with the Defense sector, citing ethical issues, they remain credible and sometimes unavoidable partners to develop effective AI tools. At the same time, by making this choice, the loss of control over industrial data could represent an unacceptable risk in a context as strategic as Defense.

Nevertheless, more and more startups are offering innovative, high-performance applications and services that can even rival the digital behemoths in very specific areas. The latter benefit from technical and social factors (such as open sourcing, cloud computing, collaboration, funding from major groups) that are favorable to their development.

By choosing to partner with start-ups, Defense increases its ability to maintain control over the developed technologies and retains greater agility to adapt an application to the context. However, the

small size and lack of resources of start-ups may slow down the progress of projects, or even prevent their technical solutions from attaining sufficient maturity so as to be safe to use in battle.

Finally, fundamental research remains the main source of scientific discoveries. Collaboration between universities and research centers combines their strengths to federate and stimulate excellent studies in many fields. Nowadays, AI is a particularly dynamic academic field of research, as recent progress continues to attract significant public and private funding.

Defense partnership with researchers and leading universities in AI - the French CNRS is the European organization which has published the largest number of articles on AI since 1960 - allows for the development of internal expertise and also plays a role in monitoring technology. This long-term investment is not viable in industry in either the short or medium term.

As a result, armies have to turn to solutions that are adapted to both the need and the relative importance of the data to be transferred to the Cloud: the "build or buy" choice remains a highly strategic issue.

The impact of digital technologies means that the traditional industrial Defense base must be expanded

On the one hand, Defense cannot turn away from its traditional industrial Defense base, which is the basis for the development of any military armament and a factor of national sovereignty. On the other hand, these industrial experts cannot compete with the Information Technology (IT) players in the AI field. The search for hybridity between the industrial and world of hi-tech expertise seems to be the most relevant solution which would provide high-performance, secure and fast-to-implement applications. For example, Thales announced, on December 8, 2020, a collaboration with Google Cloud to provide private companies and public organizations with the ability to securely migrate sensitive data to public, hybrid and private Cloud-based IT infrastructures. The collaboration provides a solution for managing and storing encryption keys that is fully controlled by the "customer", ensuring a fully secure transfer to the Cloud.

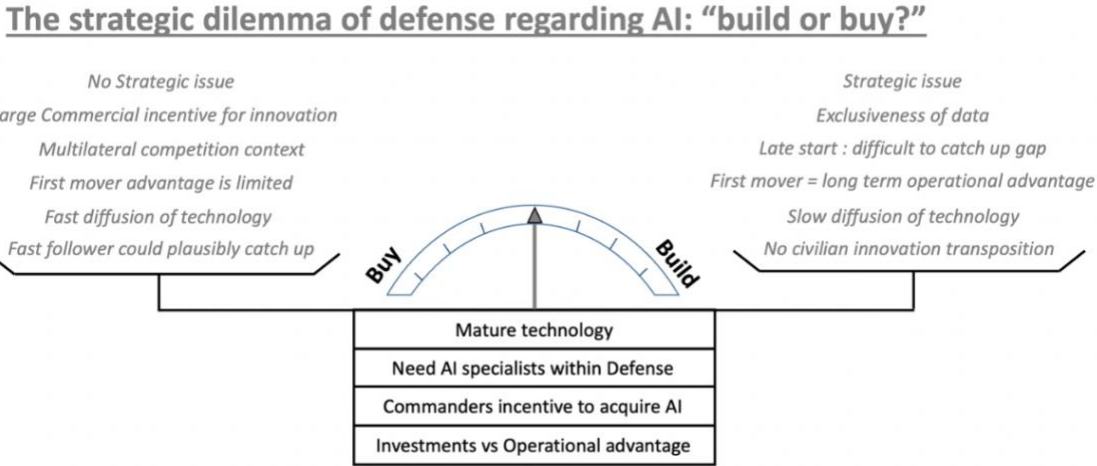
If the Defense industry is moving towards this model of partnership, which appears to resolve the issue of data privacy by securing access to sensitive data, the key to success will rely on resolving legal issues. Indeed, the place where data is stored is fundamental in terms of data sovereignty: a Cloud services provider will only be subject to French obligations if the data center is located in France.

As part of the development of massive data processing technologies of a strategic nature in connection with AI, Defense has launched a project to acquire a national Cloud Computing infrastructure, Artemis, which aims to create an ecosystem that encourages civilian companies (SMEs, start-ups and research laboratories) to bring their AI-based creations to maturity as technology usable within the armed forces.

This desire for national independence within the framework of the development of tools integrating AI for its armies would enable France to reinforce its technical and operational superiority in a very specific niche: the artificial intelligence analysis system for geospatial data of Preligens is the appropriate illustration of this strategy. The start-up, specialized in satellite image analysis, offers an application that combines state-of-the-art image processing and machine learning techniques that automatically aggregate information from various sources, such as imagery (ROIM), signals intelligence (ROEM) or open source (ROSO), concerning critical sites of interest, to acquire information superiority. Algorithms, such as Preligens offers, could play a significant role in greatly improving the situational awareness of headquarters, to keep them updated on the fast-changing situations of the battlefield. It would give the French Defense sector a crucial advantage within the field of intelligence and could even enhance how the military will operate in the future.

These developments of a national approach should be complemented by a "buy" approach, when the applications are not of a strategic nature or if France needs to fill a capacity gap. In terms of HR tools, for example, the turnkey solution for purchasing algorithms, Cloud Computing capabilities and data

migration could be completely outsourced to a private company. Beyond the significant savings that this solution brings, it enables the concentration of all human and financial energies on high value applications.



France is one of the leading hotbeds for digital start-ups

While France does not have any digital-related companies that can compete with GAFAM, the start-up sector has been dynamic over the last decade. The French social model is largely responsible for encouraging their creation and fostering their growth through the establishment of an attractive ecosystem.

Adapting traditional business regulations to the digital world and introducing incentive plans dedicated to innovation are the main levers of this new dynamic. Moreover, in addition to traditional European investment aid, BPI France offers a number of tax breaks that correspond to the different stages of an innovation project to encourage entrepreneurs to take risks.

France has also created a digital ecosystem to encourage the establishment of incubators and accelerators in order to foster the creation and development of digital businesses. The creation of the Station F campus, in 2017, illustrates this desire to bring ambitious ideas to life: its campus hosts a startup zone with many workstations, event spaces, and 26 international programs. The incubator also provides services essential to the development of startups: investment funds, a manufacturing laboratory, 3D printers and public services. Microsoft and Facebook have signed partnership agreements and are also present on the campus to offer dedicated services to startups.

Defense is also trying to capture the attention of innovative digital companies.

If French companies do not appear to be inherently opposed to working in Defense for ethical reasons or at the risk of their corporate reputations, a certain reluctance exists nonetheless, notably because of a lack of knowledge of this specific sector, perceived as mysterious by many civilian companies. There is also an apprehension to engage in a long cycle within a market often considered closed and with excessive bureaucracy. However, Defense represents a market that is robust to changes in cycles, and which generally better resists crises. The health crisis caused by the Covid-19 is a perfect illustration of this paradigm.

As part of its overall strategy to foster innovation, the French Ministry of Defense offers a number of financing mechanisms for innovative companies whose technologies are of interest in the Defense sector. These solutions, based on public contracts, are of two types: subsidies or investments. They are

dedicated both to the support of critical and strategic companies for Defense (Definvest) and to the development of cross-cutting technologies of companies in the IT sector (R&D Rapid, Defense Innovation Fund), even those whose innovations might not seem directly applicable to Defense.

These funding solutions contribute to the development of an ecosystem of interest for the Defense sector and aim to create a knock-on effect for private investors who might be reluctant to invest in the Defense or tech sectors. France has chosen to support high-potential innovation projects dedicated to Defense, with a priority dual nature (civil and military applications) so as not to penalize the development of companies with a unique market.

After several years of experimenting with these funding mechanisms, the French Defense ecosystem needs to evolve in two fundamental directions:

- Limiting subsidies to investing more in order to create markets for French companies, following the American example;
- Transforming the relationship between start-ups and industrial Defense groups, which must develop a new model of partnership rather than maintaining the traditional customer-supplier one that penalizes their respective growth.

C. Governance

The definition of a data strategy and the development of an ecosystem conducive to the development of AI must allow digital governance to become clearer. Indeed, the latter is currently distributed among different actors and services at all levels of operation within Defense. As its evolution and deployment has been gradual over the last 20 years, the dilution of responsibilities and the scattering of financial and human resources in this area is a logical consequence. However, this hinders the conduct of large-scale projects and leads to development redundancies, which, in a constrained budgetary context, is harmful to the entire system.

This governance must be materialized through the allocation of human and financial resources, and above all through the dissemination of a strong digital culture. At the same time, interoperability must be considered in order to anticipate sovereignty issues in the event of a coalition commitment.

1. The development of sovereign AI systems induces a skilled and trained human resource

Advances in AI are fast and the market is very dynamic. However, depending on the type of data and its classification, it will be impossible for armies to constitute a fully representative sample of data to validate the product and declare it operational ("full ops"). Therefore, the development of sovereign systems created end-to-end by Defense will have to be considered. This requires the acquisition of resources, and in particular an identified and much sought-after human resource.

AI experts are located at different levels of competence and training, and therefore at different levels of the hierarchy:

- Data analysis technician or "labelist": requires limited training of a few weeks and is aimed at characterizing the data according to its future use; this does not require any particular computer skills but rather in the field of the data in question. This type of training would be aimed at officers or senior NCOs in staffs from levels 1 to 3 initially and then at level 4;
- Data scientist/engineer in ML: building models to drive system decisions;
- Data engineer/data architect: management of resources and the technological structuring of data;
- Data analyst: managing and working with data in terms of information or data that can be activated or used.

These professions would be nothing without the existing IT base, including network technicians and administrators, Cloud administrators, developers and programmers, IT project managers, systems security specialists.

This AI-centric approach should not neglect the interdisciplinary approach specific to each project: linguistic engineers, lawyers, sociologists, psychologists, but also military personnel from armies and services to express and specify needs and constraints. Interdisciplinarity facilitates the broadening of skills and expertise according to the project envisaged and helps avoid the possible pitfalls of the many biases (cognitive, data).

Highly sought-after in the job market, this human resource requires that several types of recruitment and training be considered: active military personnel, operational or citizen reservists, civilian personnel. The possibilities are numerous but must take into account that the labor market in this field is extremely competitive.

As a result, the Defense sector must be attractive in terms of remuneration and professional interest. Aligning itself with civilian salaries seems difficult without creating new statuses; however, one can envisage systems of hiring bonuses, financing of training with in-service links and financing of research and dissertations (doctoral students) as already mentioned above. In addition, it is also necessary to gain the interest of young engineers by presenting projects from the angle of general interest and the meaning given to the action, in particular to attract potential operational reservists or citizens.

Finally, it is necessary to diversify the origins of recruitment to ensure both a good knowledge of the needs and the operational environment without sacrificing technical expertise and permanence in the position, which allows long terms knowledge and the establishment of lasting relationships with civilian and military partners.

More generally, the users of these systems will not be computer scientists, and it is vital for armies to develop their digital tools by focusing on their "usability", i.e. how user-friendly they are. The young generation that is very accustomed to the digital world in their daily lives will have no difficulty in mastering a system if the interface and operation are conceived of as a smartphone application, hence the need for an approach focused on users and their characteristics. Appropriation could be more difficult for Digital Immigrants, the older generations whose use of digital has necessitated a transition, one that is not always successful.

Moreover, as mentioned above, one cannot separate the development of information systems containing AI and data (software or algorithm) from the IT infrastructure (hardware or network, storage). Consequently, the links with the DGA, the Digital Defense Agency (AND), the AID, the Joint Directorate of Infrastructure Networks and Information Systems (DIRISI), the General Directorate of Digital and Information Systems (DGNUM), the AND and its Information Systems Directorate (DSI), the IT departments of armies and services, Cyber Command must be solid and clearly defined to develop AI in concert with the appropriate hardware and software environment. This requires an integrated approach to AI and digital technology in general in the armed forces, within an organization that centrally manages the deployment of digital technology. This means allocating the means to achieve this and a radical change of culture in this area.

2. A digital culture remains to be built

Over the past decade or so, the cyber threat has opened up a new field of conflict and highlighted the growing vulnerabilities of our weapons systems, made more powerful and more precise by the potential of computer systems. Our growing dependence on these facilities, with the need to remain at a high level of technology, is forcing us to rethink security in terms of the soldier and their equipment.

However, security is only the tip of the iceberg of digital culture. Data and their labeling (cf §III A), the understanding of systems containing AI and digital facility like cyber security are all areas related to digital technology that will become ubiquitous within Defense. For the young generation qualified as "digital natives", it will be easy to enter the digital environment since they have been immersed in them since they were very young and can no longer do without their smartphone in their daily life. For other age groups - the "digital immigrants" - the sociological and psychological issues are different. If we add

the observation that in our European societies the relationship with the machine or the robot is more anxious than in the United States or Japan, we can guess that the diffusion of the "smartphone" is a major cause of anxiety.

This cultural transition is necessary and urgent in order to change the way armies view the digital world, which today is seen more as a constraint, a vulnerability and a vector of loss of autonomy. It is only possible if we consider with objectivity and pragmatism the current needs and ambitions, the level of investment of our allies, partners and competitors in the field and, as a corollary, our own. The implementation of culture will require the demonstration of both the efficiency of these systems and their high level of reliability. The pilot projects mentioned above are a good support for these demonstrations. The very structure of armies, vertical and hierarchical, if effectiveness is proven, will then allow the dissemination of these capabilities and their use under the conditions for which these systems were created. However, the feedback process must not be forgotten in order to draw a clear and objective assessment of these systems.

3. A budget allocated to develop sovereign programs

The allocation of financial resources is necessary to achieve the ambitions and projects that Defense has set itself in terms of digital technology.

However, these decisions must be accompanied by a clarification of the digital governance that is currently distributed among the various players in the digital Defense sector, including the DGNum, DGA, DIRISI, Comcyber, AND, armies and services. Each army and service has very specific needs linked to its operational vocation as well as its daily missions. However, the place of digital technology in our societies, in our work tools and on the battlefield should force Defense to rethink this place and to consider digital technology as a field in its own right, where operational superiority, communications, the use of systems and efficiency in daily operations are at stake.

In 2018, French Minister of the Armed Forces Florence Parly explained the ministry's digital ambitions: "To [...] be at the forefront of digital transformation, the Ministry of the Armed Forces has set itself three objectives: to guarantee operational superiority and information control in theaters of operation; to strengthen the efficiency of support and facilitate the daily work of personnel; and to improve relations with citizens and the attractiveness of the Ministry.¹⁶" It is within this dynamic that the DGNum and the AID were created in 2018, followed by the AND in 2020.

Reporting to the Director General of Armament, the creation of the Defense Digital Agency, dating to November 30, 2020 and taking effect in 2021, will implement the digital strategy defined by the DGNum. Among other things, the DNA will enable information systems to be rationalized and managed by domain and specialty. The aim here is to avoid development and/or purchase redundancies between departments and armies for identical or similar needs.

This transition to a growing digital role can only be made gradually, in successive stages, so as not to slow down or disrupt the deployment of major projects already underway. However, it is unavoidable in order to rationalize, bring coherence and fully integrate the different components of the digital environment on which Defense depends, both in terms of organic functioning and operations. The evolution of mindset, combined with the allocation of financial resources, will lead this transition towards greater efficiency in the digital realm with the goal of maintaining a modern Defense system commensurate with national ambitions.

These ambitions include the desire to commit to a multinational military coalition, which raises the issue of system interoperability with our allies.

¹⁶ Chloé Benoît, « la DGNUM : vers une révolution numérique du ministère des Armées », July 2018, <https://www.usine-digitale.fr/article/la-dgnum-vers-une-revolution-numerique-du-ministere-des-armees.N718119>

4. Interoperability "by design"

During the conference on AI and data on December 3, 2020, the French Defense's Engineer General Jérôme Lemaire, head of the AI and Big Data (DGA) mission, declared, referring to governance and interoperability: "There are as many data governance systems as there are countries¹⁷." The message is clear, and the question of the interoperability of information systems, with or without AI, is one of great consequence.

In accordance with the White Paper on National Defense and Security (LBDSN) and the latest Strategic Review (2017), France wishes to position itself within Europe and NATO as a framework nation and coalition leader. This implies having interoperable means at all levels, particularly in the area of operational communications. Interoperability must therefore be included from the system design stage as an element to be taken into account in the specifications in the same way as resilience, robustness, security, data and its labeling, and the related physical structure requirements.

If we consider this political and strategic will and the sensitivity of the data regarding both secrecy and ownership, it is clear the interoperability of artificial intelligence systems is inherently difficult. Obviously, it is conceived and implemented differently according to the types of AI systems and their sensitivity: an AI system that performs predictive maintenance, image analysis or decision support, for example, does not present the same challenges because the security issues are completely different. However, taking into account the classification of military data, the development of interoperable systems is rendered particularly complex and is inextricably linked to the ambitions of States. Consequently, in the first instance, and assuming that this desire for interoperability is shared, the only conceivable solution lies in the development of ad hoc tools with the data that the States concerned will agree to supply and share.

The framework in which interoperability seems most feasible is that of a stable and perennial alliance such as the UN, NATO or the EU, one able to define a regulatory, normative and procedural environment for the data in order to make it usable by a common interoperable system.

Another opportunity is to continue and expand the development of projects in an already existing partnership such as the MGCS with Germany or Great Britain under a kind of Lancaster House agreements that would be extended to AI. This would also allow for the identification of possible constraints and limitations.

IV. Conclusion

AlphaDogFight is an excellent example of demonstrating the power of AI against humans with a competition of leading manufacturers on the subject. However, the conditions of the confrontation, in simulation, should not be lost sight of, in the sense that it is not yet an AI and a pilot opposed in real conditions and there is still research to be done before reaching this level of maturity.

In an increasingly unstable geopolitical context, and faced with competitors and allies who are investing massively in the field, French Defense is determined to seize the opportunities offered by artificial intelligence and the technologies they bring together in order to maintain a certain operational credibility.

To do so, it must prepare for the changes and developments that such a breakthrough will entail. The legal and ethical corpus must still evolve at the international level to define the possible limits of use of these systems; nevertheless, reflecting on the topic leads to an understanding that allows a controlled use of AI.

Concerning implementation, the reality of armies and services has allowed progress to be made on the subject but there is still a long way to go and measures must be taken in the very short term to avoid

¹⁷ Lemaire J., Defense Engineer General, Direction Général de l'Armement, (12/03/2020), « Les données de l'Intelligence Artificielle dans le champ de bataille ».

falling behind. The collection, processing and storage of data are the basis for the deployment of a powerful and effective AI for uses that will have been determined according to the interests of the armies.

At the same time, a Defense A.I. ecosystem must be built so as to enable dynamic, responsive and efficient development, based on sovereign and outsourced resources according to the determined usage. The "make or buy" issue must be resolved by distinguishing strategic projects requiring development by the Defense sector from others that can rely on the traditional Defense industrial base and on start-ups that would complement it in a timely manner.

Finally, digital governance needs to be rethought by spreading a culture that would make digital no longer a constraint but a means that is totally integrated into the soldier's environment. This will require the recruitment of an expert human resource, but also a profound change of mindset regarding the use of digital tools in general. This will lead to a clearer governance of the digital world within armies, and perhaps even, in the long term, a definition of a Digital Army that would evolve in this new environment of confrontation and vulnerability.

V. Appendix 1: business model for AI integration within Defense ecosystem







New digital technologies have profoundly transformed our societies for several decades and AI could even be a catalyst in the future. Man will have to face and coexist with artificial intelligence in combat, but also in his daily life. This paradigm shift initiated by the digitization of the world imposes a strategic adaptation of relations between the civil and military in the context of the acquisition of digitized equipment. From now on, it is civilian industry that is driving the technological researches and development that are transposed, once mature, into Defense systems.

However, if there is a consensus identifying AI as a technology that will become unavoidable, many companies are still reluctant to embark on this adventure, as the digital transition of a company is unique, non-linear and requires many financial and human investments.

The Business Model Canvas¹⁸ is a universally used tool for those companies that wish to invest in the digital field. The canvas is used to transcribe, in a simple way, the business model of a company and finds all its relevance during a phase of reflection on the launch of a new product or service. In a context of digital transformation, where civilian industry is leading the tempo of innovations, it seems wise to study the integration of AI in weapon systems, following the example of a business case, focusing mainly on operational excellence and the value proposition.

¹⁸ Business Model Canvas were initially proposed in 2005 by Alexander Osterwalder

Business Model for AI integration within Defense

<p>Key Partners </p> <p>Traditional Industrial Defense Base</p> <p>Innovation Defense Agency and Digital Defense Agency</p> <p>Fundamental R&D (Universities and Research centers)</p> <p>Start-ups</p> <p>Allies (Europe, NATO, US, UK)</p>	<p>Key activities </p> <p>Warfare skills</p> <ul style="list-style-type: none"> - operational superiority over an enemy on the battlefield whatever the environment - Defense needs to be adapted to the digitalization of society and battlefield 	<p>Value proposition </p> <p>AI is a lever to better/faster understand, anticipate, optimize and ultimately decide</p> <p>AI to better understand:</p> <ul style="list-style-type: none"> - improve situation awareness (Detect/Reco/Identify) - identify trends inaccessible to humans <p>AI to better anticipate:</p> <ul style="list-style-type: none"> - provide predictive insight - computing capabilities inaccessible to humans 	<p>Customer/user relationship</p> <p>Permanent dialogue to define needs, utility & usability of systems</p>	<p>Beneficiaries </p> <p>Operational excellence of a Modern Defense</p> <ul style="list-style-type: none"> - operational superiority - interoperability - optimize the characteristics of a medium-size technological army <p>“Customer Experience”</p> <ul style="list-style-type: none"> - military leaders
<p>Cost Structure</p> <p>Public funding</p> <p>Export sell</p> <p>Norms & Interoperability</p>	<p>Key resources </p> <p>AI Experts</p> <p>Equipment</p> <ul style="list-style-type: none"> - adaptation for AI integration - AI environment (Clouds) - scalable weapon design <p>Sustainability + Management of processes & systems</p> <p>Data to feed algorithm</p>	<p>AI to optimize:</p> <ul style="list-style-type: none"> - optimize human workload - optimize processes, flows and resources <p>AI at the service of doing good:</p> <ul style="list-style-type: none"> - better discrimination of combatants and non-combatants - better control the effects of weapons <p>➤ Foster the military leader's decision</p>	<p>Channel/deployment</p> <p>Define pilot projects (few)</p> <p>Develop a Data strategy</p> <p>Create a Digital ecosystem for armament procurement</p> <p>Develop a Digital Culture</p> <p>Adapt organization and governance</p> <p>Requires Force commanders' incentive</p>	<p>French Diplomacy</p> <ul style="list-style-type: none"> - credibility relying on a high level of technology of the Defense <p>French Economy</p> <ul style="list-style-type: none"> - Sustain French Tech - Develop new market for the Industrial Defense Base
<p>Cost Structure</p> <p>Public funding</p> <p>Export sell</p> <p>Norms & Interoperability</p>		<p>Revenue Stream </p> <p>Export opportunity</p> <p>Use of armed forces, defense manpower and resources on a Just-Need basis</p> <p>Operational superiority</p>		

VI. Appendix 2: press release announcing the contribution of AI in armed operations

Press Release

The mastery of AI, an instrument of European victory in the Cyprus conflict

The European intervention Makarios, under French command, allowed the liberation of Cyprus in 13 days. The mobilization of AI-assisted technologies was a determining factor in the logistical support and the conduct of operations, the fruit of 8 years of investment provided by the French armies, betting on emerging technologies with high potential.

Paris, May 21, 2026 - Fanny & Brice/Service d'Information et de Représentation Publiques des Armées - The Makarios military operation, launched on February 4th to liberate Cyprus from Turkish occupation, is the first to be conducted using AI technology. This technological mastery gave a decisive advantage to the European forces, which were outnumbered and allowed a lightning capitulation of the Turkish forces, entrenched east of Nicosia.

During preparations for the land operation, artificial intelligence algorithms overwhelmed the Turkish intelligence services with information, preventing any analysis of sea and air movements, thus leaving the Coalition complete freedom of maneuver all the way to the island's outskirts.

The force commander, General Fanny Pelurty, believes that *"AI, integrated with the various satellite observation and listening systems, coupled with the operational-level information processing algorithms, was decisive," because it provided "an almost perfect representation of the battlefield, ensuring optimal precision of each air strike on the Turkish forces, while avoiding collateral damage."*

In the field, the perfect synergy between the combatants and their information processing tools gives a decisive advantage over an adversary frozen by the Coalition's multi-domain combat dynamics. Commander Brice Marttiero, IA Advisor, explains the advantage conferred by these embedded tools in the platforms and in the staff: *"The algorithms deployed free operators from ancillary tasks to dedicate all human cognitive resources to decision making, considerably accelerating the OODA (Observation, Orientation, Decision, Action) loop at all levels. This enables us to anticipate opposing maneuvers thanks to an instantaneous representation of the battlefield and to immediately use the weapon system best suited to each target."*

The use of AI is the result of a strategic orientation rethought 8 years ago within the French Defense Procurement Agency (DGA). The result of collaboration between anticipation, research and the military, it has highlighted European logistical power: supplying forces at the right time to maintain an intense operational tempo that stifles the enemy. The power of predictive maintenance algorithms makes it possible to increase the availability of equipment on the battlefield by 15%, compensating for the numerical inferiority of the European forces.

At the signing of the armistice on February 15, Army Chief of Staff Thierry Bosser said: "The adoption of artificial intelligence in French Defense is the result of financial and human investments made Minister of the Defense Florence Parly, as well as the Defense Innovation Agency. This has led to the development of four pilot projects deployed during Operation Makarios, which have shown their effectiveness. These predictive maintenance, decision-support, satellite image analysis and listening systems, used in perfect synergy with the combatants and staffs, enabled us to outperform our adversary. They are a perfect illustration of the success of the digital transformation of armies.

Bibliography

- Everstine, Brian W., "Artificial Intelligence Easily Beats Human Fighter Pilot in DARPA Trial", August 20, 2020, <https://www.airforcemag.com/artificial-intelligence-easily-beats-human-fighter-pilot-in-darpa-trial>.
- Midgley, G., Lindhult, E. (2017), "What is systemic innovation?", Research Memorandum 99, University of Hull.
- Christensen, Clayton M.; Bower, Joseph L. (1995), "Disruptive technologies: catching the wave", Harvard Business Review.
- Garcia, R. and Calantone, R. (2002), A critical look at technological innovation typology and innovativeness terminology: a literature review. Journal of Product Innovation Management, 19: 110-132.
- Pfaff C.A. (2019) "The Ethics of Acquiring Disruptive Technologies: Artificial Intelligence, Autonomous Weapons, and Decision Support Systems", PRISM Singularity VOL.8 NO.3: 128-146.
- Goasduff Laurence, "2 Megatrends dominate the Hype Cycle for Artificial Intelligence, 2020", September 28, 2020, <https://www.gartner.com/smarterwithgartner/2-megatrends-dominate-the-gartner-hype-cycle-for-artificial-intelligence-2020/>.
- Clausewitz C.V (1832) "Principles of War", the Military Service Publishing Company, translated and edited by Hans W. Gatzke in 1942.
- Endsley M.R. (2000) "Situation Awareness analysis and measurement", CRC Press.
- Stephanie Mundubeltz-Gendron, "Intelligence artificielle : 4 enjeux, 5 atouts et 1 mission selon Edouard Philippe", september 2017, <https://www.usine-digitale.fr/editorial/intelligence-artificielle-4-enjeux-5-atouts-et-1-mission-selon-edouard-philippe.N585443/>.
- Chloé Benoît, "la DGNUM : vers une révolution numérique du ministère des Armées", july 2018, <https://www.usine-digitale.fr/article/la-dgnum-vers-une-revolution-numerique-du-ministere-des-armees.N718119>.
- Lemaire J., Defense Engineer General, Direction Général de l'Armement, (12/03/2020), « Les données de l'Intelligence Artificielle dans le champ de bataille ».