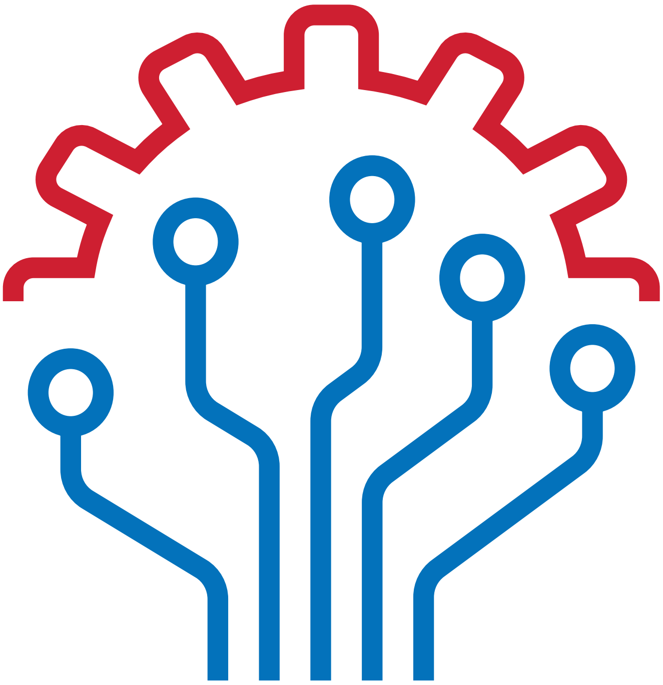
ARTIFICIAL INTELLIGENCE IN SUPPORT OF DEFENCE



"The path we choose is that of responsibility, of protecting both our values and our fellow-citizens while embracing the amazing opportunities that artificial intelligence offers."

Florence PARLY

Report of the AI Task Force
September 2019

Liberté • Égalité • Fraternité
RÉPUBLIQUE FRANÇAISE

MINISTÈRE DES ARMÉES

CONTENTS

INTRODUCTION

Artificial intelligence (AI), a concept which originated in 1956, is now a reality in the lives of most people. Recent advances in deep-learning algorithms combined with an explosion in the amount of available data have paved the way for a wide variety of AI uses which are likely to have far reaching effects not only on our economies and the way we work but also on global strategic balances.

Some see AI as a vast source of progress for humanity that will relieve people of tedious chores and increase their cognitive capacities while improving their health and access to knowledge. Others perceive only the threats that AI already poses to our democracies and our privacy, and could pose in the future to our jobs or respect of our ethical values.

Between immortality, transhumanism and the end of the world heralded by the reign of robots, artificial intelligence is the nexus of all hopes and fears and, in some cases, fantasies.

It is also a focus of fierce global competition. Almost every week, major powers and private companies, some of them with very substantial economic clout, announce new breakthroughs and massive new investment in AI. The race for talent is under way and, while the excellence of French scientific education is widely acknowledged, it does not always benefit our country or our business community enough. **That race is so swift and the prizes at stake so great that any falling away would be fatal.**

Although AI technologies will play a key role in future operational superiority, they are not an end in themselves as far as the armed forces are concerned, but rather a means to help them continue to perform their missions. These are to guarantee France, now and in the future, its capacity to assume responsibilities for peace and security in the world, and to protect its territory, its citizens and its interests while acting in strict compliance with international humanitarian law (IHL) and without unnecessarily risking the lives of service personnel.

The French armed forces cannot therefore stand aside from these developments, at the risk of missing a major technological turning-point and losing the operational superiority they currently enjoy. Within the framework of the national strategy initiated by the President of the Republic, this document sets out the Armed Forces Ministry's artificial intelligence strategy. It presents an ambitious but pragmatic roadmap, consistent with our country's values, which will enable the entire ministry – armed forces, administrations and support services – to benefit from the significant progress being made in this highly promising field.

1 - ARTIFICIAL INTELLIGENCE AND DEFENCE

1.1 THE STATE OF PLAY IN THE AI REVOLUTION

1.1.1 A flourishing field

Artificial intelligence – a catchy term but one that many experts consider inappropriate because it lends human characteristics to machines – covers a range of notions which change over time.

Artificial intelligence is defined in the Official Journal of the French Republic[1] as an "interdisciplinary field of theoretical and practical study which seeks to understand the mechanisms of cognition and thought and use a combination of hardware and software to imitate them in order to assist or replace human activities". As such, the boundary of AI shifts in response to scientific progress and the human perception of "smart" tasks. 30 years ago, the first computer proofs of geometrical theorems and the first systems for human-machine dialogue were seen as being at the cutting-edge of AI. Now we regard them merely as conventional algorithms which make use of raw computing power.

Whatever its scope, AI remains a means and not an end in itself. It does not replace people, even though it may perform certain tasks for them.

More specifically, artificial intelligence is used in applications which aim to:

- *detect* and *recognise* data (text, voice, images, video, etc.) or even *predict* future data;
- *seek correlations* between data in order to deduce a generic form of behaviour from them or on the contrary flag up abnormal behaviour;
- *optimise* highly combinatorial problems such as logistical flows or flight paths;
- *reason* from symbolic data in order to *deduce* or *diagnose*.

From a technical standpoint, artificial intelligence has two main branches: *symbolic approaches* based on reasoning (rules-based systems), and *connectionist*

[1] Artificial intelligence vocabulary. OJFR no. 0285 of 9 December 2018, text no. 58.

approaches closer to empiricism, based on learning from large databases (neural networks).

Advances over the last decade, such as mass data processing, algorithms using deep neural networks, increased computing power and the use of graphics processing units (GPU), have had a ripple effect, resulting in the rediscovery of the different AI techniques. These effects have been amplified by the sharing of open-source algorithms and by research challenges which have spurred spectacular progress in object recognition and autonomous navigation.

Despite this undeniable progress, however, AI technologies are still far from robust in unknown environments that are difficult to generalise. Their results can sometimes be hard to explain or lead to gross errors. This explains why most AI applications today remain limited to elementary or non critical tasks. In the defence sphere, AI technologies will have to make further progress before they can be used in a controlled way.

progress has been made in tumour image analysis, achieving higher levels of recognition than even the most experienced professionals.

Most of these achievements stem from major digital players, especially American and Chinese, which have access to what really fuels AI: the vast mass of data that their customers provide to them free of charge at each interaction. Having initially sought to know their customers better in order to enhance their products and services, these actors are now using their very deep pockets to pursue greater ambitions, such as driverless cars, smart cities and personalised healthcare. Their products set the standard, and the sheer extent of their use cases makes them attractive to the military, especially in the many dual-use applications. As in the digital sphere as a whole, the defence sector does not necessarily blaze a trail but takes advantage of advances in civilian uses, adapting them to its own particular needs where necessary.

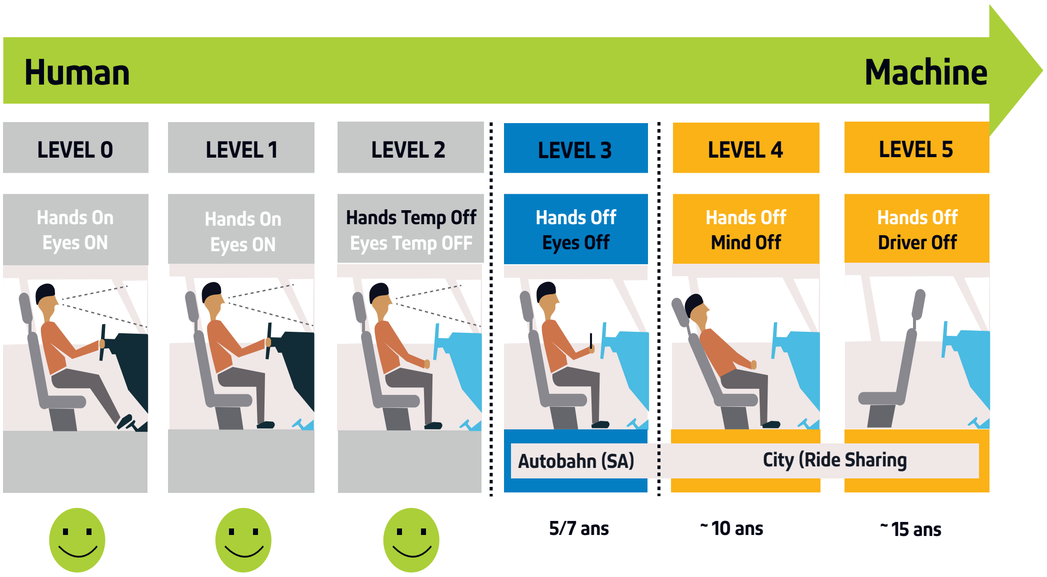


Figure 1 – Estimate by Gardner and PwC of how autonomous vehicles may evolve (on the basis of studies carried out in 2017).

1.1.2 Dual and defence-specific uses

While the general public may have been impressed by the success of Alphago or the sporting prowess of Boston Dynamics' robots, AI is not widely used in practical industrial and commercial applications. Quickest to take up these burgeoning new technologies have been the e-commerce, marketing, finance, industrial maintenance and human resources sectors. For private individuals, the first applications using non-structured data, such as voice and image processing, are invading home speakers and smartphones. In the health sector, very significant

The armed forces must thus strike the right balance between benefiting from the things that major private – and often foreign – digital firms can offer, without becoming dependent on them, while developing their own military applications. As far as the least specific applications are concerned, especially tools for administrative management optimisation, financial consolidation and human resources management, the Armed Forces Ministry's data and needs are similar to those of any other ministry or large firm. The civilian market already develops and offers products for such uses.

Military operational systems, on the other hand, have important specific features, whether in terms of tasks to be performed, the type of data to be manipulated (infrared images, radar or sonar data, etc.) or performance and robustness requirements. Civilian actors do not develop methods for processing these types of military data.

In addition, military operational systems have features which, with the exception of certain critical systems in areas such as aviation and banking, are rarely to be found in civilian applications:

- the systems are often **embedded and deployed in open and unknown environments;**

- they must meet **stringent requirements in terms of latency and robustness** but generally have **low energy resources** and **limited-speed links** between themselves or with data centres;

- they must be systematically **pre-qualified** before being brought into service in order to ensure they perform as required.

In order to address these specific features, the ministry will rely extensively on the existing algorithm base, mostly available in open-source, except in specific cases where particular attention will be paid to the risk of reverse engineering. However, the more defence-specific the use cases or the data processed, the more the ministry will have to invest in designing and configuring algorithm chains for itself.

1.1.3 Abundant potential to support operational superiority

Taking advantage of this momentum, military AI applications are being developed incorporating aspects such as computer vision, smart robotics, distributed intelligence, natural language processing, semantic analysis and data correlation.

Strategists and military commanders, in their operational and organisational responsibilities, must be able to take advantage of AI and turn it into a decisive factor of operational superiority. The aim here is to gain speed and room for manoeuvre from better recognition and/or detection of targets and hitherto unknown dangers in the field, from faster and better targeted military action, and from deception actions while ensuring compliance with the laws of war.

Understand more fully, anticipate as always, take decisions more quickly

AI favours a new way of processing data which, combining speed of operation with massive cross-analysis, identifies underlying trends and singularities much more effectively and quickly than a human being could. AI may therefore be expected to bring a fuller and swifter understanding of situations in increasingly complex and interdependent areas of operation.

AI will help to better anticipate the adversary's manoeuvres and optimise operational processes (guidance, gathering, exploitation and dissemination of intelligence). Well-calibrated, it will procure many advantages, for example in the assessment of a threat and optimisation of the response to it.

The time saved through AI in accessing and processing data will allow more scope to explore the options under consideration when planning and conducting operations. AI will make a decisive contribution in relation to weak signals, which may herald important changes, thus helping to significantly reduce the element of surprise. Feedback data processed by AI will also be integrated into the decision-making process, providing iterative enhancement.

The improved understanding of the situation that AI provides will help to validate options for modes of action and hence step up the pace of decision-making.

AI is therefore capable in the short term of ensuring that the armed forces' decision-making processes have the necessary operational superiority to give them the upper hand over many types of adversary.

Give service personnel better protection

In addition to supporting the conduct of operations, AI will benefit service personnel. Through massive processing of health data and an extension of health monitoring, AI will identify risk factors related to the environments and working conditions of the armed forces and propose appropriate protective measures to limit the impacts on the health of service personnel.

Integrated into simulation, AI will also help to improve the training of units and individual training paths, especially when it is combined with augmented reality in the context of war gaming, serious games and immersive virtual environments.

Robotics will not only enable service personnel to stay at a distance but also offer better self-protection, as for example with operations in contaminated environments, fire-fighting, mine clearance on land or at sea and defence against drone swarms.

The better protection of combatants offered by AI is not limited solely to the operational sphere, since AI will also be of significant assistance in promoting respect for the values of IHL. By supporting a better assessment of the operating environment at tactical, operational and strategic level, AI will greatly help to:

- improve discrimination between combatants and non-combatants;

- enhance proportionality by controlling the effects of weapons according to the threat;

- guarantee that action is determined strictly by need.

Contrary to certain popular misconceptions, AI has a potential which, properly managed and controlled, will help the French armed forces to take better account of the fundamental principles of the law of armed conflict.

Free up personnel from ancillary tasks

In addition to the optimisations described above, artificial intelligence heralds a far-reaching change in the preparation and conduct of operations. AI should ultimately assume many ancillary and repetitive tasks, freeing up personnel from time-consuming chores and allowing them to concentrate on high value-added tasks. In the chain of command in particular, AI will enable staff officers to focus on thinking and decision-making.

In space observation, image interpreters will be able to efficiently exploit the flow of information, which is much larger with CSO satellites than with those of the previous generation. In operations, systems equipped with AI will be able to act as back-up to combatants. For example, piloted aircraft may be accompanied by UAVs to support them in their missions.

It is generally accepted that 80% of human error occurs during routine tasks. If those tasks are carried out by AI, the risk of human error due to repetitive and mechanical actions will be reduced.

Optimise flows and resources

Artificial intelligence supports the implementation of predictive models which help to foresee and optimise the ministry's logistical flows, technical management of fleets of equipment and scheduling of the associated maintenance, financial commitments and recruitment. The use of predictive analysis to optimise flows and resources is a particularly mature AI application which also has a strong dual-use aspect. Consequently, even taking into account the specific features of military operations, AI can quickly bring significant benefits in this type of application, as the work carried out at SGA's Labo BI shows.

1.1.4 A revolution that is not without threats and risks

Because AI will be inherent in all systems, the threats associated with its use are the corollary of the opportunities it affords and could affect all spheres of interest, from intelligence, command and engagement to maintenance, support and the condition of personnel (state of mind, morale, etc.).

AI technologies are not yet mature enough to upset power relations or change the nature of warfare. It is a fast-moving field, however, and the steadily decreasing cost of the technology suggests that new modes of action and disruptions of uses or thresholds will emerge in the short term. Being easily accessible, especially as a result of the diversion of commercial technologies or the use of low-cost robots, these new threats will soon become much more pressing.

The fears they raise include:

- the possibility that adverse AI will be able to predict our modes of action, depriving us of the element of surprise;

- the paralysis of our command capabilities as a result of the neutralisation, deception or diversion of our technologies;

- the extension of influence operations and actions targeting the circulation of information (disinformation, undermining media credibility, fake news, etc.);

- the change of scale and the proliferation of high-frequency hostile actions in the cybersphere (coordinated attacks, deception actions, etc.).

Competition, levelling and disruption

Artificial intelligence can destabilise existing balances by fostering arms-related competition that may result in technological disruption or the levelling of strategic positions.

The technological race under way in AI is part of the now-resumed arms race. This could be amplified by the dual-use nature and extension of the technological applications of AI. As the scope of future AI applications is so vast, most countries perceive that the established hierarchy of military power can be altered to their advantage. Without necessarily being at the cutting-edge across the entire spectrum of AI technology, the mastery of certain key technologies may be enough to upset the established order.

AI can level strategic positions, especially if used asymmetrically. Non-state actors can cleverly exploit future civilian off-the-shelf technologies, using innovative means to prepare tactical surprises. Certain countries may back AI technologies that offer new means of destabilisation, such as cyber attacks or disinformation using AI-enhanced audio or video manipulation software to create deepfakes, or behavioural analysis software applied to opinion groups. This raises the risk of blurring the line between reality and fiction, which could undermine the political credit of democracies.

AI also lends itself to rapid incremental changes which can lead to technological disruption.

Tangible progress is likely to be made in detection, aggression and decision-making, fostering new imbalances that encourage escalation. Such scenarios could result, for example, from:

- the fear of being on the wrong side of a technological surprise;
- the temptation to strike first (pre-emptive or preventive strike);
- the rapidity of technological progress which does not leave enough political time to reach agreement on confidence-building measures in support of arms control.

Risks arising from the use of AI

The roll-out of artificial intelligence is still in its infancy and often limited to the more error-tolerant use cases. Industrial-scale AI, especially for military uses, implies more stringent robustness requirements. The technology is making rapid progress but there are risks inherent in certain techniques. Deep neural networks can still be manipulated to deceive human perception, for example by introducing differences imperceptible to the human eye into two images.

Learning techniques likewise pose various risks:

- involuntary bias, especially where learning data are not representative (e.g. ethnic bias in population data);
- voluntary bias, if a third party has been able to amend learning data or the model in order to produce an abnormal result, possibly on request;
- reconstitution of particularly sensitive learning data (reverse engineering), especially if the third party has knowledge about the techniques or learning tools used;
- opaque or not readily explicable results that humans would have difficulty trusting in critical systems.

Generally speaking, the quality of learning data is a decisive factor for obtaining robust algorithms. If learning data are non-existent, inaccessible, insufficient or unsuited to the intended use, the results obtained will not be satisfactory.

The risk of dependence on a technology which makes certain tools easier to use must also not be ruled out. Consequently, steps must be taken to maintain the skills needed to perform a mission in a resilient way and with reduced use of AI. The roll-out of artificial intelligence must therefore be accompanied by the necessary measures to avoid any loss of human skills that would make the mission difficult to perform without recourse to AI.

While certain risks associated with the use of AI, such as deception, back doors, reverse engineering and low resilience, are not specific to it, they may be less easy to detect because they are less “intuitive”. A considerable amount of research is being done into such risks, and into ways of forestalling them, and should be followed attentively and supported by the Armed Forces Ministry.

1.1.5 An international landscape which reflects major global tensions

International competition already under way

Many countries have recently released civilian artificial intelligence strategies. This acceleration and the global emulation that goes with it bear witness to the shared impression that AI expertise is an essential power factor for the future. The various AI strategies published recently reveal a global hierarchy of AI power which may be considered as follows:

- **two superpowers, the USA and China,** beyond the reach of other nations, each of which controls a vast mass of data, has an ecosystem based on powerful, global integrators (GAFA and BATX) and is in a position to use its scientific and financial resources to further increase its domination;
- **an aspiring intermediate power, the EU,** whose hardline approach to legal and ethical issues may be a strength or a weakness depending on its impact (standard-setting power underpinned by many public- and private-sector actors vs risk of having a research or entrepreneurial development policy that is too timid or hampered by excessive regulation);
- **a second circle of countries,** including France, Germany, the UK, Japan, South Korea, Singapore, Israel and Canada, which have certain advantages but not sufficient critical mass. The extent of their autonomy will depend on the leverage they can extract from the cooperations they are able to establish and the relevance of niche strategies that maximise their comparative advantages.

Strategies that reflect national ambitions

a) An essential common base: attracting talent, doing research, setting standards

Keeping home-grown talent and attracting skills from elsewhere is the first element common to these various strategies. All wish to carry out extensive basic or applied research and decompartmentalise AI applications. The technological building-blocks should thus spread from the private to the public sector, from the civilian to the military sphere, between research and industry and between the different strands of AI (complementarity). This concern is reflected in organisational strategies which seek, inter alia, to create structures that encourage such cross-fertilisation.

All countries also wish to play an active and if possible driving role in the preparation of AI standards. The production of global standards enables them to project themselves as powers helping to shape a still-evolving foundation for AI spanning technological, legal, commercial and behavioural standards.

b) Major differences over use: ethical and security aspects

These differences concern the ethical aspects first and foremost. A distinction can be drawn between actors who pay little attention to such matters and others that are more scrupulous.

There is a fundamental difference between the two major players, the United States and China. The latter can guide private-sector actors with a firmer hand and instruct them to cooperate with the public sphere, including the military. China has thus come up with the doctrine of "civil-military fusion" designed to maximise transfers between research, industry, the state and the armed forces. In the Chinese model, AI applications are firmly extended to the security sphere. Relations are more complicated in the United States, where the reluctance of certain companies to work with the Department of Defense has already disrupted certain projects, such as Maven . These social and institutional aspects are the main distinction between China and the United States.

c) Aggressive competition in the medium term

Competition to acquire the necessary resources to develop AI has already begun and is likely to become more intense. The resources in question are both intangible (capturing scarce human resources) and tangible (capturing key technologies, etc.).

1.1.6 Ethical concerns monopolised by "killer robots"

Technological development has been accompanied among all actors by an awareness of the ethical implications of AI. However, international discussions have tended to centre on the potential development of lethal autonomous weapons systems (LAWS). A Group of Government Experts (GGE) on the subject was set up under the Convention on Certain Conventional Weapons (CCCW) in 2017.

Countries are sharply divided on the outcomes that may be expected within this framework. France is making an active contribution to the debate, defending a "realistic" position: LAWS do not exist at present and a preventive ban would hinder a response to the legal and ethical challenges raised by such systems.

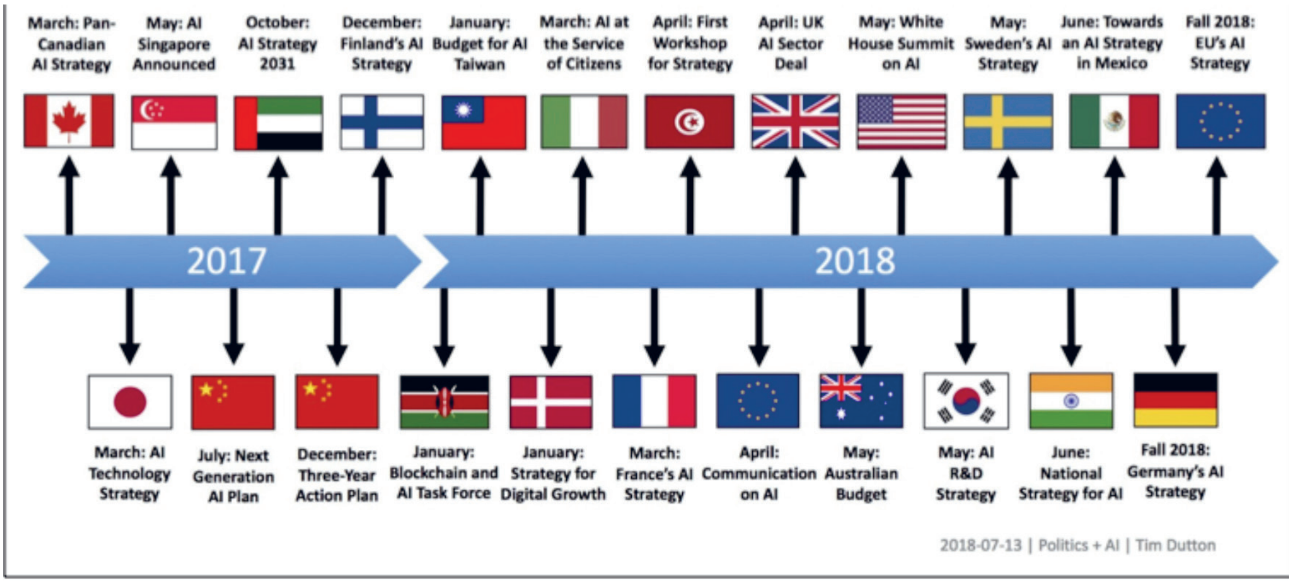

March: Pan-Canadian AI Strategy
May: AI Singapore Announced
October: AI Strategy 2031
December: Finland's AI Strategy
January: Budget for AI Taiwan
March: AI at the Service of Citizens
April: First Workshop for Strategy
April: UK AI Sector Deal
May: White House Summit on AI
May: Sweden's AI Strategy
June: Towards an AI Strategy in Mexico
Fall 2018: EU's AI Strategy
2017
2018
March: AI Technology Strategy
July: Next Generation AI Plan
December: Three-Year Action Plan
January: Blockchain and AI Task Force
January: Strategy for Digital Growth
March: France's AI Strategy
April: Communication on AI
May: Australian Budget
May: AI R&D Strategy
June: National Strategy for AI
Fall 2018: Germany's AI Strategy
2018-07-13 | Politics + AI | Tim Dutton

Figure 2 – Publication of national AI strategies

1.2 GUIDELINES FOR A CONTROLLED DEFENCE AI

1.2.1 Keep our freedom of action and interoperability with our allies

In order to preserve their superiority against adversaries with increasingly agile expertise in digital technologies, the French armed forces must anticipate the disruption that will inevitably result from AI-related technological advances.

The use of AI in weapons, information and command systems is already a major operational issue with regard to both keeping the upper hand in response to symmetrical and asymmetrical threats and remaining on a par with the lead nations in a coalition.

Our allies within a national, NATO or EU framework are themselves in the process of integrating AI into their military systems. Interoperability with our allies must be preserved by means of common standards, which are essential for the conduct of operations in coalition. The capacity to counter the effects of adversary AI will also be a decisive factor of strategic dominance, which means acquiring without delay the skills and the technologies that will enable us to keep the upper hand.

1.2.2 The assurance of trustworthy, controlled and responsible AI

Systems containing AI are intended to operate with a certain degree of autonomy. Nevertheless, it is essential for the Armed Forces Ministry to have robust and secure systems which can be trusted to assist service personnel and commanders, dispelling any "black-box" effect, while retaining human responsibility for action.

Trustworthy AI of this sort relies on rigorous systems design which must guarantee total compliance with the human-defined framework, and on the ministry's capacity to evaluate and certify such systems.

Human beings will then be able to make the most of the system and, in doing so, gain a real factor of operational superiority. The aim is to combine human judgment with the power of algorithms in order to take decisions and act clear-sightedly at an ever-faster operational tempo.

Operational performance will be superior to that of the human being or machine in isolation, or even in juxtaposition.

1.2.3 Preserve the resilience and upgradability of our systems

Robustness and resilience are critical issues in an environment where the success of engagements depends on communication networks and access to information. The French armed forces must have resources endowed with those qualities in order to guarantee the pursuit of operational objectives at all times. The robust integration of AI will provide autonomous functions that offer relevant solutions, especially where communications are limited, neutralised or impossible. That will mean validating and qualifying those functions, then adapting the medium to make it consistent with operations in a highly contested environment.

Such environments also mean that AI-equipped systems will sometimes have to operate in degraded mode. In such cases, operational units will have to be able to use the systems in that mode and retain the capacity to perform their missions effectively without recourse to AI. Forces will need regular training and exercises.

A long-term view is one of the main features of the design and acquisition of military capabilities, since many items of equipment have a lifespan of 50 years or more. For AI, an eminently dual-use technology with a much shorter development cycle, it is essential that equipment currently being designed incorporates AI-based systems from the earliest possible stage and remains upgradable over several decades.

1.2.4 Keep a sovereign core

As the 2017 Defence and National Security Strategic Review says, "expertise in artificial intelligence is set to become a sovereignty issue, in an industrial environment that is characterised by fast-paced technological innovation and currently dominated by foreign companies".

The global AI ecosystem is dominated by American and Chinese digital giants which are developing in-house capabilities as well as buying up numerous promising firms. The United States has GAFA (Google, Apple, Facebook and Amazon), Microsoft and IBM as well as the ecosystems of specialist smaller firms and startups that have grown up mainly around San Francisco and New York. In China, BATX (Baidu, Alibaba, Tencent and Xiaomi) and many startups, mainly around Beijing and Shenzhen, give the country a definite advantage.

AI also requires vast amounts of computing power, as for example in the most widely-used case of deep learning technologies, where large data sets are used to train up neural networks. This capacity is generally accessible in public or private clouds, most of which are again dominated by American firms (Amazon Web Services, Microsoft Azure, Google).

In a context dominated by foreign private or state actors, France cannot resign itself to being dependent on technologies over which it has no control. In the specific case of military AI, and in order to ensure the confidentiality and control of our information, it is essential that we preserve our technological sovereignty.

Where research is concerned, France is very well placed in global terms and often considered to be the best in Europe . Nonetheless, the process of industrialising AI and turning it into a service industry is less advanced here than in the UK, Canada or Israel, a situation which applies equally to civilian and defence industries. In order to avoid falling behind in AI technology, it is therefore essential to move towards a better balance between basic research and industrial applications while also developing comparative strategic advantages in an agile strategy of niche superiority, either alone or in cooperation.

At the same time, it will be necessary to organise data storage capacity and acquire data administration, preparation and enhancement tools within the framework of a comprehensive data policy. For critical applications such as weapons systems, it will also be essential to be able to audit the characteristics of algorithms and data that may have been used for learning purposes and to upgrade them.

While generic algorithms are available to everyone, their designers are careful to hold on to their configuration, their learning elements, their combinations and their data. Preserving digital sovereignty therefore also involves controlling the algorithms and their configuration, and the governance of data.

2 - ARMED FORCES MINISTRY ROADMAP

2.1 A ROBUST ETHICAL AND LEGAL FRAMEWORK FOR THE ARMED FORCES MINISTRY

The Armed Forces Ministry is particularly conscious of the ethical and legal issues that may be raised by the use of AI in defence applications, whether for administrative and technical tasks or for operational purposes. Ethics and law are core elements of the training received by French service personnel. The principles of international humanitarian law (necessity, humanity, proportionality, distinction) and the values that stem from a rich philosophical, historical and operational history – courage, generosity, concern for others, efficiency, responsibility and realism – are incorporated into the strict and sequenced process of planning the use of force and into a chain of decision-making for the application of force established by the rules of engagement, validated by government.

To ensure that AI-based technologies do not call these principles into question, especially the place of humans in military action, their development for defence purposes will systematically retain military commanders' responsibility for the use of weapons. France has no plans to develop fully autonomous systems where human operators have no control over the definition and performance of their missions. France will hold fast to its international commitments and continue to contribute proactively to the work currently under way in the framework of the CCCW, especially the GGE on emerging technologies relating to LAWS.

That is why the Armed Forces Ministry has decided to make comprehensive arrangements designed to inform its thinking and its ethical stance in a transparent and explicit manner.

2.1.1 A ministerial ethics committee

A multidisciplinary and permanent ministerial ethics committee will be established, focusing on emerging technologies in defence. It will ensure long-term compliance with the principles described above and inform ministerial thinking at a time when new uses of AI are emerging daily. The committee, which will be set up in 2019, will work closely with the National Ethics Advisory Committee.

Its membership, comprising suitably qualified persons from outside the ministry, will ensure the necessary balance between credibility and operational effectiveness. Able to act on its own initiative, the committee will issue advisory opinions that will be in the public domain unless the confidential nature of their subject matter makes publication inadvisable.

➢ Set up a ministerial ethics committee before the end of 2019.

2.1.2 Measures to raise awareness of the uses of AI

In order to ensure that those who have to implement AI technologies are aware of all their implications, a training and exercise phase will be introduced before systems incorporating AI functions are used operatWionally. The aim is to raise awareness among all service personnel of the benefits and risks associated with the technology. Data valorisation will be a key point of focus.

- ➢ Take steps to raise awareness among ministry staff of the use of AI, especially from an ethical standpoint.

2.1.3 Technical measures to ensure trustworthy AI

AI remains a recent and sometimes immature technology which can generate outputs that humans may perceive as aberrant. Image recognition systems, for example, based on statistical learning and the use of deep neural networks, may produce a completely wrong result or be duped by a variation of a few pixels.

There may be various reasons for these errors:

- errors of implementation stemming from learning data that are contextualised but not representative of the population as a whole;
- malfunctioning algorithms, which means that it must be possible to subject algorithms to expert appraisal before they are implemented;
- insufficient understanding of the behaviour of the hardware or software integrated into the AI system in relation to the criticality of the function.

The ministry will ensure that a "right level" of trustworthiness and robustness is assessed for each AI application. Determined according to the criticality of the functions performed, that level results from the systematic conduct of risk analysis as of the design phase. The risk analysis must help to identify which of the different functions are the most critical in order to deduce the relevant requirements in terms of development, qualification and monitoring in use.

The consideration given to AI-related risks in security studies may result in only certain techniques being chosen, according to the criticality of the function, or an insistence on human validation at certain stages of the algorithmic processing chain. These principles for trustworthy AI design form part of the ministry's chosen ethical framework.

In the longer term, the inclusion of some of these requirements in standards will help to simplify and homogenise developments leading to certification. Identified as a necessary point of focus in Cédric Villani's report , certification is an important goal. In the future, it could be performed by a trusted service provider with recognised and up-to-date expertise. The requirement level for systems acquired from non-French providers will be comparable to that demanded of a domestic supplier.

- ➢ Incorporate the specificity of AI into operational security analyses for weapons systems and other developments for the ministry's needs in order to determine the right level of trust and ensure that human control is maintained.

2.1.4 The need to construct international standards

Standardisation plays an important role in the recognition of levels of performance and quality in many sectors. Standards make it easier to draw up specifications (a single standard can cover a large number of individual requirements) and help manufacturers to position themselves on export markets, given that most countries use the same standards in their own contracts.

Although expressed in terms of performance requirements, standards are not entirely independent of technical solutions. Stringent performance requirements or specific features in the definition of the standard may make it difficult for our manufacturers to achieve the necessary level or require new work on design and development. In contrast, high-performance systems cannot be discerned if a standard is too lax.

Standardisation work in artificial intelligence could focus on the robustness of algorithms and methods for preparing learning bases and developing and testing software modules incorporating AI. Merely verifying performance is not enough: the requirements must also extend to the software engineering process. This method is already in use for critical software in the aeronautical, automobile, nuclear and railway industries, for example. However, the methodology and current standards for the safe operation of critical software are not suited to certain families of AI technologies such as neural networks. Critical software experts and AI experts will have to work together on these issues.

Work on drafting voluntary AI standards started in 2018 via AFNOR, the French standards organisation, which has set up a national standardisation committee on AI technologies . Internationally, many countries are taking part in the work carried out by the ISO, especially those in the first two circles of AI. The focus at this point is on the definition of a common vocabulary, systems architectures and the establishment of a programme of work. Other working groups will probably start up in sectors where specific standards and regulations apply, such as the aeronautical and automobile industries.

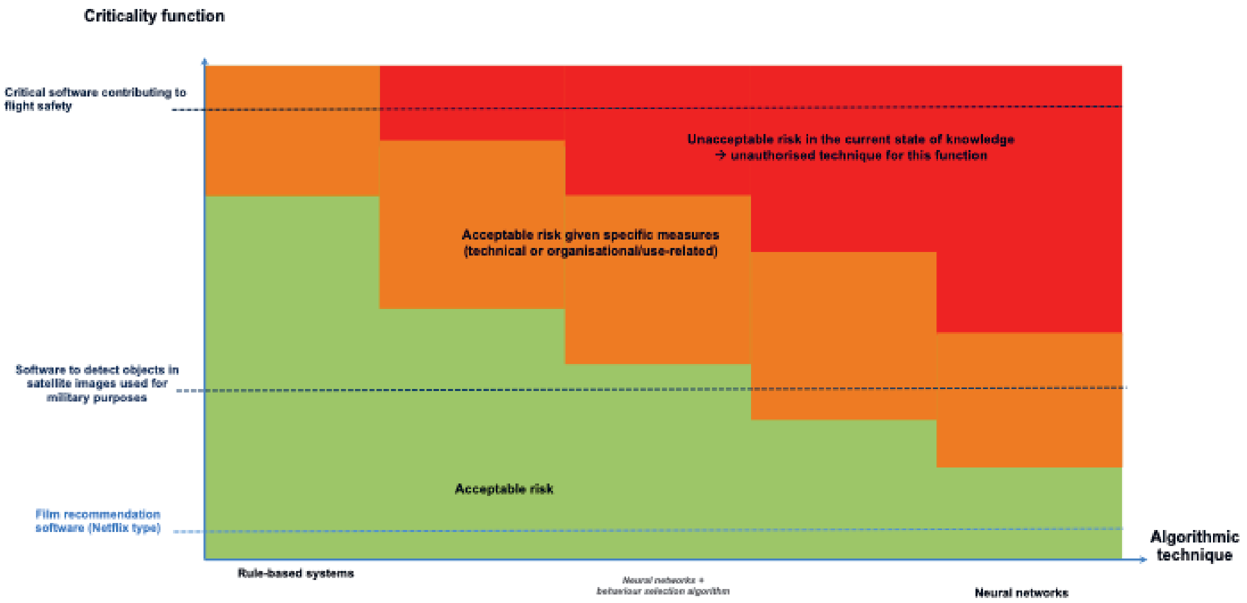


Figure 3 – Risk level of AI-based algorithmic technologies according to criticality

➢ Play an active part in civilian and military work on standardisation and encourage major defence contractors to do the same at national and international level.

The Armed Forces Ministry must also take steps to explain the issues at stake in the integration of AI into critical systems, including civilian systems, insofar as they raise issues of ethics, law, industrialisation and accountability which need to be discussed with our partners.

➢ Circulate France's defence AI strategy and oversee its implementation both at interministerial level and in international discussions on critical systems that incorporate AI.

2.2 DATA AND HARDWARE: THE NECESSARY FOUNDATION FOR THE SUCCESSFUL DEVELOPMENT OF AI

On the basis of the principles described above, the ministry is drawing up an operational roadmap for the development of AI suited to military needs. It is based first and foremost on data management and valorisation, computing power and storage capacity.

The ministry's digital strategy expresses the data challenge in terms of "using new digital technologies to share, exploit and valorise data" in order to "make the masses of data collected by the armed forces meaningful". DGNUM, the Directorate General for Digital Technology, introduced a data policy for the ministry in 2018, with the aim of:

- identifying existing data sources and ensuring their quality and completeness;
- taking steps to create sets of correctly annotated data;
- organising storage capacity while acquiring data administration, preparation and enhancement tools;
- defining data exploitation models by analysing use cases according to occupational needs, creating databases with standardised sharing interfaces that make it easy to obtain proofs of concepts and perform learning tasks.

The search for procedures to provide data for training AI algorithms or testing them on our real data must be carried out with determination. It will be an essential precondition for studying and understanding the algorithms and evaluating them for operational use.

2.2.1 Govern the data

Having access to reliable, up-to-date data implies exercising control over the data lifecycle from capture to valorisation, including production, processing and storage. This is a key issue for the Armed Forces Ministry. It means that data must be regarded as a strategic asset and supposes a policy underpinned by the construction of a genuine data governance system.

The twin purposes of data governance are to ensure control of the ministry's assets and to create the climate of trust in which they can be shared, respecting the requirements of regulatory compliance, security and right use. Ultimately, it must guarantee optimum exploitation of data while alleviating the data-entry burden on units. The current silo governance model, based on segregation by type of use, must move towards a cross-cutting model that allows for the exchange of data between reference systems and gives the armed forces visibility over activity.

Action has already been taken at three levels:

- strategic, in order to provide a coherent overview of the data. This involves constructing the ministry data map, identifying sensitive data with regard to priority issues, organising data collection, defining accessibility rules and overseeing quality assurance policies;

- operational, in order to draw up a "highway code" for data. This involves defining and implementing the rules for sharing each type of data and defining procedures for exchanges between producers, owners and consumers while ensuring the traceability and proper conservation of data. It is a vital condition for rationalising data entry and exchanges in information systems and a factor of coherence for the construction of shared indicators;

- organisational, to determine roles and responsibilities. This involves identifying the actors involved within the scope of the data, defining roles and responsibilities and organising the associated comitology.

Governance must be founded on two pillars:

- a data-oriented architecture whereby data can be stored, collected, processed, exploited and circulated and those capacities made available securely both to ministry entities and, where they need to be shared, to trusted industrial partners.

  ARTEMIS will ultimately provide a framework for trialling all these needs. In the meantime, the POCEAD platform will provide an initial technical capacity for valorisation and a first methodological building-block for data governance;

- a genuine data culture which first and foremost raises awareness among all actors, not just specialists. A secondary aim is to achieve a better understanding of the issues of right data use and the transparency requirement it implies, including the ethical dimension. It will also involve anticipating needs for the skills without which a data policy of this type cannot work.

The aim of expanding control over data as a strategic ministry asset calls for a multi-year action plan in three phases:

- phase 1 (2018/2019): construction of an initial technical and methodological capability for data, mostly based on POCEAD, defining the ministerial governance framework and the operational tools to implement it, as well as determining the necessary levels of subsidiarity for data collection, quality assurance and exploitation;

- phase 2 (2020): consolidation of the technical capabilities and methodological foundation, drawing on feedback from POCEAD and use cases trialled with ARTEMIS;

- phase 3 (2021): organisational maturity of data governance, in phase with the roll-out of ARTEMIS, in response to the ministry's strategic challenges.

This policy will have to be accompanied by a revision of uses and of methods for designing future information systems, based in particular on the introduction of data-oriented architectures.

2.2.2 Protect personal data

There is a crucial distinction between personal data, from which a person can be identified, and non-personal data. The collection and exploitation of data on a massive scale cannot be envisaged without strict compliance with the prevailing personal data legislation, especially the General Data Protection Regulation (GDPR).

2.2.3 Anticipate the collection and exploitation of operational data

Data collection and storage is necessary not only for valorisation but also for successive learning phases. Our systems must therefore include capabilities for recording data from sensors. Some of these data will be processed locally for learning or test purposes. Such records are also a means of traceability in the event of malfunction.

Applications that involve merging and mining distributed data also require substantial telecommunications capacity in order to limit successive syntheses and fusions which impair the richness of the information contained in the raw data. Once the flow rate is imposed, the optimised distribution of processing will help to ensure that the information contained in the exchanged data is used to best advantage.

2.2.4 Acquire specific computing power and storage capacity

In addition to data, some applications that use AI require access to very substantial computing power and storage capacity. Cloud computing is one technology that helps to meet those needs.

With the cloud, substantial amounts of storage capacity and appropriate computing resources can be allocated very quickly according to needs (a Rafale, for example, produces 40 terabytes of data per hour).

Cloud technology increases infrastructure resilience by quickly and dynamically reallocating resources in the event of malfunction (if a hard disk fails or a server is lost, for example, environments can be reconstructed rather than repaired).

The cloud offers security and reliability. By enabling the automation of actions and the deployment of resources via scripts, it minimises human intervention and hence the associated risk of error or threat.

Offering standardisation and automation, the cloud is thus a means of optimising the ministry's effectiveness by improving collaborative tools and valorising data (entered once, used as required). It is also an essential way of facilitating exchanges with the outside world.

The Armed Forces Ministry's cloud strategy is entirely consistent with the central government cloud strategy based on concentric circles:

- an internal or private cloud, with access restricted to the ministry alone, that will provide direct support to operations. It is operated by DIRISI (Joint Directorate for Infrastructure Networks and Information Systems);

- a dedicated cloud that will combine security with the use of innovative technologies, where resources will also be privatised but localised with a trusted operator. Integrated into the ministry's cyberdefence structure, it will be the subject of a specific industrial strategy with trusted operators and offer collaborative storage space to the ministry's partners. In the longer term it could meet the specific needs of other bodies looking for a secure cloud, such as other ministries, DITB actors, operators of vital importance, etc.

- an external or public cloud that will help to capture innovation by making shared resources available to all.

The built-in synergies between the services provided by each circle will make code more easily portable from one circle to another and facilitate access to innovation on the internet.

Lastly, the ministry will provide defence cloud cybersecurity via DIRISI and CALID (the defensive cyber warfare analysis centre) in compliance with the recommendations of ANSSI, the French National Cybersecurity Agency.

➢ Implement the ministry's cloud strategy in order to ensure the storage, availability and accessibility of data, including classified data, tailored to needs and in compliance with security requirements.

Other disruptive technologies should also be mentioned because they will directly impact performances and capacities based on AI.

➢ Get involved in the governance of quantum and high-performance computing projects.

2.3 PRIORITY AREAS OF FOCUS FOR THE MINISTRY

The combination and convergence of artificial intelligence, robotics, augmented reality, systems networking and the internet of things will play a key role in future defence systems and make a significant contribution to operational superiority. As well as implementing AI in operational systems, the armed forces must be able to use AI more widely in their digital transformation process and explore its contribution to and potential implications for all their activities.

In the following section, promising applications from a military standpoint have been classified according to seven strands:

- decision support in planning and execution,
- collaborative combat,
- cyberdefence and influence,
- logistics, support and operational readiness,
- intelligence,
- robotics and autonomy,
- administration and health.

The aim of each strand is to give the armed forces new capabilities, i.e. coherent sets of people and equipment, organised, trained and supported in accordance with a doctrine, with a view to operational use. This definition, common to all the armed forces, is summarised in the French acronym DORESE, which corresponds to doctrine, organisation, human resources, equipment, support and training.

A significant investment of more than €700 million in equipment and studies is already planned over the period of the current Military Planning Act, giving an annual average of a little over €100 million.

2.3.1 Decision and planning support

In addition to stored data, two other aspects are essential in order to construct this element: an infostructure that will provide a foundation for the development of specific applications, and the practical development of those applications (data-centred information system). Standardised interfaces (API) will ensure that the applications are compatible. The rest of this section focuses on the practical aspects of decision support in planning and execution.

Decision support must be available in command centres (C2) at strategic, operational and tactical level, before (anticipation and planning), during (execution) and after the mission (evaluation). It means that data must be desegregated and cross-referenced because C2 tools will manipulate previously inaccessible data from very different types of sensors and sources (intelligence, cyber, maintenance, health, etc.). Learning-based mass data processing will be performed mostly at dedicated data centres. Once the AI module has been trained, it will be deployed to remote systems (operational or tactical) through transmission via telecommunications networks.

In a very practical way, AI will help to filter, enhance, exploit and share data and provide help with manoeuvres, and hence offer combatants informed choices so that they can take decisions more quickly while reducing uncertainty (humans still take the decisions). Human-machine interactions will benefit from the contribution of AI, partly through augmented human-machine interfaces and partly through optimised cooperation between units, systems and combatants (including human/robot cooperation).

Decision support in planning and execution

During the planning phase for a battlegroup operation, each vehicle or group of vehicles is allocated a mission and a recommended itinerary according to its type, mobility and action capability, and identified threats in the intervention zone.
During the operation, the vehicles may at all times have a shared view of the tactical situation (map updated in real time) and hence synchronise their manoeuvre. Using their perception functions, the vehicles can also detect changes in the environment in relation to the initial situation and initiate a revision of the initial manoeuvre. The assignment or reassignment of tasks, calculation of itineraries and automatic processing that enable changes in the environment to be detected are typical cases of the application of operational AI research..

2.3.2 Collaborative combat

The coordination of systems and operational entities is recognised as a key factor for accelerating the tempo of a manoeuvre in military operations in all environments. The "collaborative combat" concept emerged in the early 2000s to underline the importance of improving the exchange, sharing and exploitation of information for tactical purposes. Artificial intelligence can make a contribution, whether to data mining for the purposes of anticipation, immediate response or coordinated conduct of the action, or to the smart management of flows to ensure optimum use of the available flow rates.

Data mining in this context mainly involves sharing, merging and cross-referencing information in order get a better picture of the tactical situation. Other aspects include improving the response time to threats or even preparing the allocation of effectors and the distribution of tasks within elementary units.

In flow management, AI can help to select the best compromise between centralised and decentralised processing, route the different flows appropriately, facilitate interoperability among heterogeneous systems and prioritise flows.

Collaborative combat

Use case: Management of radio frequencies in operation and in coalition
During a ground operation in coalition, French, British and German infantry units are tasked with securing a geographical zone, for example in an urban environment. They use new-generation radio sets for their communications. The infantry use a national wavelength to communicate amongst themselves within the same unit, or a coalition wavelength between units of different nationalities to enable communication between radio sets made by different manufacturers. Radio frequencies are pre-assigned between the coalition countries before the operation (frequency spectrum planning). With smart networks, each radio set, capable of analysing the locally available spectrum, will be able to identify new resources for its own use. For example, if a partner-nation unit is operating momentarily in a deep indoor environment, such as underground galleries, it could potentially free up its frequencies, which could then be used by the French forces or another partner.

2.3.3 Cybersecurity and digital influence

Cyberdefence is an area in which AI will probably have a decisive operational impact. Promising AI applications are:

- analysis of traces in a network to detect intrusion or malicious activity;
- anticipation of threats, based on available sources of information (open source);
- measurement of system resistance levels;
- countering digital influence.

The work envisaged during the current military planning round focuses on the development of an ecosystem that will favour short-cycle innovation.

To that end, the ARTEMIS structure will be used to help detect and anticipate attacks, since it will enable the data to be captured and processed by AI. A dual-use issue, it will be the subject of interministerial cooperation (e.g. AI challenge in the cyber sphere).

Digital influence will benefit from extensive synergies with the civilian sector in areas such as marketing engineering and counter-measures against disinformation campaigns.

Cyberdefence and influence

<u>Use case:</u> Detection of cyber-attacks
A cyber-attack is not necessarily a quick strike. They are generally phased operations in which several weeks or months may elapse between the initial intrusion and the final effect (data theft, sabotage, etc.). Efforts to counter cyber-attacks are based on a strategy which combines robust architectures (which make the attacker's actions more complex and hence slows them down) and the capacity to detect successful attacks before their effects can be felt. For that purpose, data generated by information systems activity are collected by a large number of sensors placed on networks, in servers and in terminals, whether the activity is usual (user login, sending of messages, etc.) or high-risk (virus detection, identification of malicious network traffic). This mass of data is examined at a Security Operation Centre. From raw data, AI helps to identify what is normal behaviour and what is characteristic of an attack.

2.3.4 Logistics and operational readiness

AI applied to logistics and maintenance is without doubt one of the areas with the most scope for dual-use applications. The benefits of using AI technologies in these activities may be envisaged in the short term, as the civilian sector has already started to implement them. AI offers operational opportunities in the following areas:

- greater supply-chain efficiency as a result of fluidifying transport flows;
- optimised maintenance scheduling;
- better knowledge and management of equipment availability through predictive maintenance and the optimisation of preventive maintenance;
- automation of certain tasks (warehousing, maintenance, orders, etc.);
- personalised technical training.

In the aviation sector, the F4 standard for the Rafale, ordered in early 2019, will have maintenance features designed to improve aircraft availability. This AI application is currently being examined for the next MRTT standard, following on from the planned civilian-aircraft upgrades.

Logistics and operational readiness

<u>Use case</u>: Differentiated and predictive maintenance
AI algorithms will help to better analyse technical issues and systems or subsystems data collected via sensors in order to improve the assessment of failure risk. Individual analysis of items of equipment and detail parts will lead to the scheduling of differentiated maintenance operations.
There will no longer be an overall maintenance cycle for the same fleet, but a differentiated maintenance cycle for equipment according to actual use, since wear and tear can differ according to type of use. This will help to optimise maintenance costs since certain parts will be replaced less often.
AI algorithms will support the implementation of predictive alerts on items of equipment. Certain recurring operations will not need to be performed systematically but only in the event of a predictive alert. It will also be possible to anticipate the risk of severe damage to certain monitored systems or subsystems. Better anticipation will result in better scheduling of activities and use of equipment.

2.3.5 Intelligence

The amount of intelligence data to be processed is constantly increasing. The challenge is to exploit the data increasingly effectively with finite human resources. This involves using AI to automate processing and optimise the cross-referencing of multi-source and multi-domain data with the ultimate aim of refocusing the processor on high value-added functions.

Intelligence

Use case: Smart data mining
The quest for information superiority, necessary for the success of operations, acquires a new dimension in a hyperconnected world where information of interest is drowned in an unceasing flow of exchanges and where attempts to exert influence are numerous. In order to detect events of interest within this mass of data and extract all relevant information about adversary organisations, human analysts must be supported by AI algorithms that:

- *initially filter the most relevant data ("recommendation");*
- *pre-process them (automatic translation, detection of individuals in an image, etc.);*
- *detect anomalies or recurrences that indicate suspicious activities;*
- *cross-check public information with military sources in order to detect disinformation attempts.*

2.3.6 Robotics and autonomy

*By placing means of perception and action at a distance, robots and drones dispense human beings from having to perform tasks summarised by the abbreviation **3D: dull, dirty and dangerous**. With the advent of more compact vectors and sensors and high-performance telecommunications, the armed forces already use robots and drones for tasks such as mine clearance and observation, even if the need for constant remote control can limit that use.*
On the ground, robotics and better human-machine interfaces are key aims of the SCORPION programme. For example, mule robots capable of following a human leader will soon be available.

Robotics and autonomy

Use case: Multi-robot cooperation, planning and automatic allocation of tasks to different systems
The aim of multi-robot cooperation is to leverage the capabilities of robot systems in all types of mission. In reconnaissance, an aerial drone can act as a remote sensor in order to increase a ground robot's observational scope, enable it to anticipate obstacles or infiltrate nooks and crannies inaccessible to the ground platform. In surveillance, the use of several automatically coordinated mobile robots can provide better coverage of the site to be monitored, permanently reducing blind spots while maintaining a degree of unpredictability in patrols. If multiple intrusions are suspected, sentry robots can also divide up inspection points between them in order to respond more quickly. When crossing a hostile area, a drone swarm is more likely to reach its target than a single robot, even if some members of the swarm are hit. AI pervades these multi-robot cooperation capabilities through multi-agent planning and coordination and by merging observation data. The coordination of movements within a swarm is also often derived from automatic learning techniques.

2.3.7 AI in support services

The General Secretariat for Administration has carried out forward-looking studies of the nature of administrative work over a ten-year time horizon, incorporating AI technologies such as data processing and analysis, voice recognition, natural language processing, sensors and software robots. A number of areas of focus have been identified in order meet the cultural and organisational challenge this represents:

- decision support and predictive analysis in order to programme, simulate or optimise the consumption of resources (headcount, payroll, budget and accounting, fluids management);

- automation of repetitive and time-consuming tasks, using software robots for transactional flow processes (HR, account closure controls, invoice processing);

- connected sensors in infrastructure for automatic data collection, property monitoring and predictive maintenance purposes;

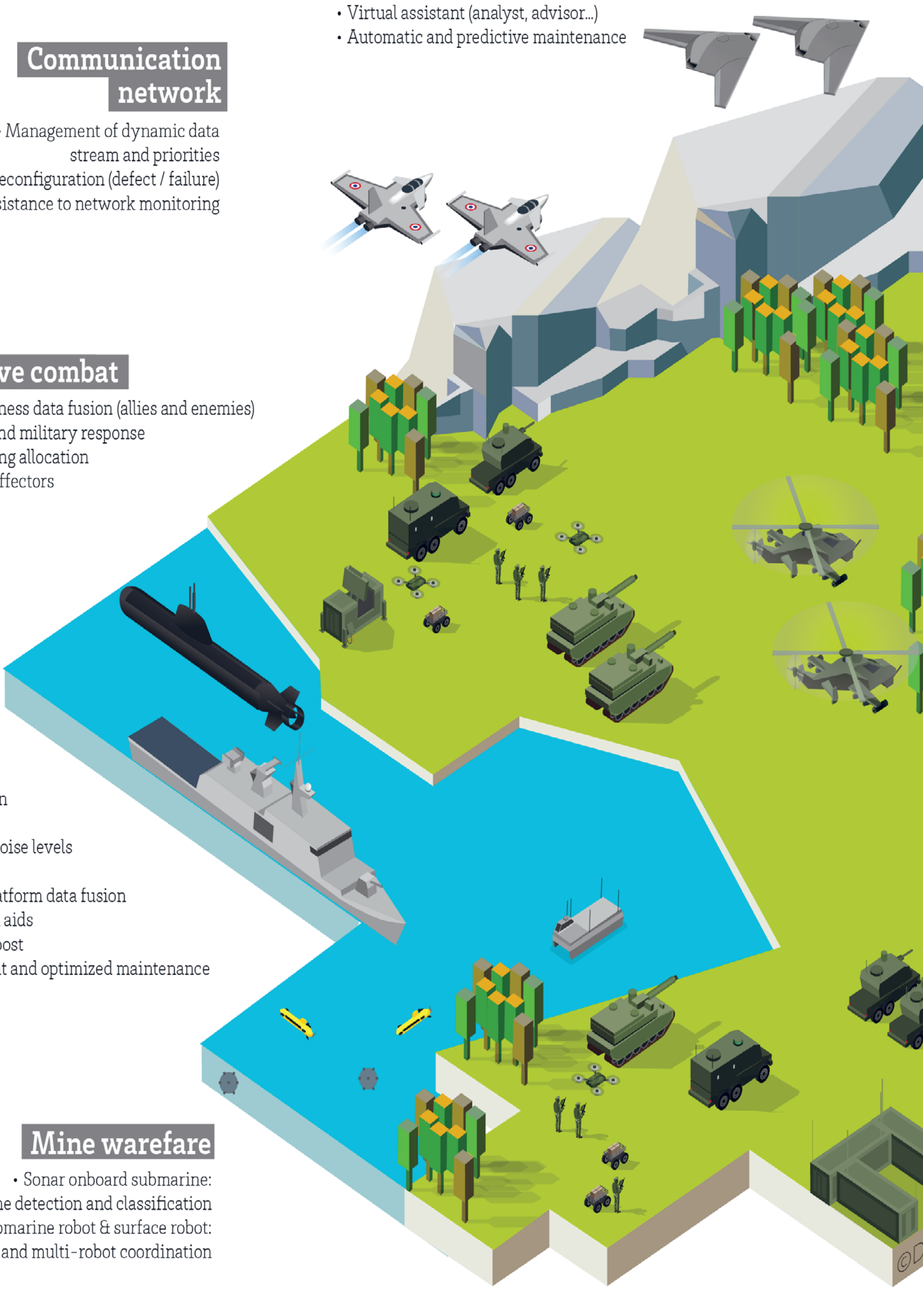
- augmented agents or users, using chatbots (natural language and voice commands) to treat FAQs, provide guidance, find relevant information and automatically produce documents and suggestions from existing content;

- new recruitment models, with automated methods of analysis derived from the behavioural and cognitive sciences, mobility prediction, etc.

AI has the potential to facilitate automation and control. Potential use cases concern cross-cutting issues such as process optimisation, management of relations with users (estimation of requests, simulations, use of virtual assistants to support frontline staff or interact directly with users), the targeting of sovereign controls and the automatic detection of anomalies. The benefit of automation is a renewed focus on core administrative tasks and service provision, relieving staff and managers of time-consuming, lower value tasks. The aim is to give them more time to provide advice or expertise or take decisions in a context where humans and machines are complementary.

Artificial intelligence

Serving the forces to boost the performance of operational systems



Combat and transport aircraft, helicopter

- Multimodal natural dialogue
- Crew monitoring and adaptive HMI
- Virtual assistant (analyst, advisor...)
- Automatic and predictive maintenance

UCAV

- Dynamic and m
- Automatized pe to environment
- Adaptive syste

Communication network

- Management of dynamic data stream and priorities
- Automatic reconfiguration (defect / failure)
- Assistance to network monitoring

Collaborative combat

- Situational awareness data fusion (allies and enemies)
- Aid for mobility and military response
- Automatic targeting allocation amongst several effectors

Submarine and navy ship

Sonar and radar:

- Stealthy target detection and classification
- Adaptation to various noise levels

Combat system:

- Multi-sensor, multi-platform data fusion
- Maneuver and decision aids
- Multimodal command post
- Opportunity assessment and optimized maintenance

Mine warfare

- Sonar onboard submarine: mine detection and classification
- Submarine robot & surface robot: Overall monitoring and multi-robot coordination

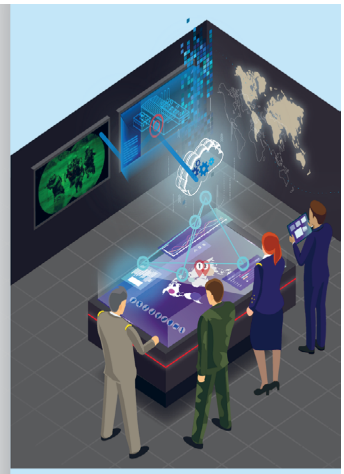
Land robotics

- Automatic sensing
- Semi-automatic navigation in complex environment
- Human-robot task sharing
- Robot – UAV Collaboration

Armoured vehicle

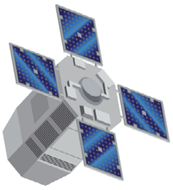
- Optronics implementing obj detection and classification
- Multimodal natural dialogue
- Threat anticipation and dec
- Opportunity assessment and

Figure 4 – Operational capabilities that can benefit from AI



Command Post

onitored itinerary generation
erception and sensor adapting
tal conditions
m reconfiguration



ISR drone, aircraft and satellite

- Relevant zones and objects detection
- On-the-fly replanning of zones of interest
- High level command orders

Connected soldier

Intelligence

- Automatisation of big data exploitation
- Multi-source data fusion
- Weak signal detection
- Data mining and summarization

Cyberspace

- Cyber-attack attempts detection
- Weaknesses analysis
- Threat analysis and anticipation
- Assistance for cyber operations (defense and offense)

Training

- Simulators with realistic enemy behaviors
- Adaptive personal training

Command

- Situational awareness data fusion (allies and enemies)
- Aids for planning and decision

e

ect

ision aids
d optimized maintenance

11 applicative families

- Planning and decision aids
- Optimization of armaments
- Human-machine interaction
- Enhanced training
- Sensor optimization and sensor networks
- Data processing and data mining for Intelligence
- Optimized Cyber
- Intelligent networks, flows and storages
- Robotic systems
- Mission monitoring and assisted maintenance
- Enhanced medicine

DGA

Liberté • Égalité • Fraternité
RÉPUBLIQUE FRANÇAISE

MINISTÈRE
DES ARMÉES

The General Staff has also carried out forward-looking work on health. Using AI-enhanced tools to collect and process biometric and medical data during training and operations will help to enhance medical support for military personnel. Embedded or not, these tools can:

- improve the health of military personnel on a day-to-day basis by assisting medical staff in their diagnosis and the provision of healthcare;

- optimise the conduct of operations by providing relevant information on personnel management (fatigue, stress, crew rotation);

- identify long-term risk or protection factors for the health of military personnel.

2.4 GOVERNANCE AND ORGANISATION

2.4.1 Define and coordinate the ministry's actions

The goal pursued is the controlled and accelerated roll-out of artificial intelligence in the armed forces, administrations and support services. Achieving it requires governance specific to the ministry. It will be based on three levels: a central core and two concentric circles.

➢ Create a Defence Artificial Intelligence Coordination Unit (CCIAD), attached to the Defence Innovation Agency (AID), with a dozen members tasked with coordinating the ministry's action to promote AI.

The ministry's competence for AI will be structured around a Defence Artificial Intelligence Coordination Unit (CCIAD) within the Defence Innovation Agency. The CCIAD's role is to facilitate the implementation of AI, coordinate projects and initiatives, and organise and oversee cross-cutting tasks such as technology and industry watch, coordination of the ecosystem, work on methodology and input into interministerial work. The permanent, multi-disciplinary team will comprise a dozen experts under the oversight of a project manager who is also the ministry coordinator. They will report to him or her and keep close links with the various actors in their original entity, where they are expected to promote the policy and coordinate actions. The members of the first circle will also cooperate with this pilot unit.

First circle

The first circle plays a highly active part in driving and coordinating AI-related activities in the various entities. Its members are the CCIAD's contacts in ministry bodies, initiators of use cases specific to each environment and mediators of best practice. The circle thus plays a key role in ensuring that the system works efficiently and in promoting an AI culture within the ministry.

It includes:

- the AI coordinators of the armed forces, administrations and support services;

- the leaders of cross-cutting actions that may involve AI, such as leaders of actions relating to ethics or the legal framework;

- the leaders of linked thematic groups.

Second circle

The purpose of the second, wider circle is to implement the guidelines and initiatives that originate with the CCIAD and the first circle. Second-circle members regularly provide feedback on their progress and on any needs for support or guidance.

The second circle comprises the leaders of projects and actions which incorporate an AI solution. They are:

- for the Defence Procurement Agency (DGA), an AI architect or AI expert who will join the team of any weapons operation that has an AI module or any upstream study associated with AI;

- for the armed forces, administrations and support services, officers leading experiments in labs, the forces or induction and training bodies such as officer training schools.

The DGA has created a new data sciences and artificial intelligence branch (DIA), whose experts and architects will constitute the ministry's key resources in AI core engineering.

Implementation of the governance model

This umbrella structure chaired by the ministry coordinator comprises the armed forces, administrations and support services, given that the data aspect will continue to be treated within the framework of the ministerial data committee. It will organise and monitor work, consider new actions to be taken with various timescales and share information on developments in technologies, uses, the ecosystem and ongoing actions.

The ministry coordinator will also report on the progress of the overall project to the Defence Innovation Steering Committee, chaired by the DGA, which will fix the broad guidelines.

2.4.2 Foster a proactive culture of AI use in the ministry

The ministry's senior management and the various echelons of operational command must be made appropriately aware of artificial intelligence. This will give them a better understanding of its use and enable them to judge the plans for significant investment in AI.

Ministry staff must be AI literate. The digital passport introduced by DGNUM may in the future include elementary knowledge of the subject. AI literacy will contribute both to work on uses and to successful roll-out when they become effective.

For that purpose, the CCIAD will be responsible for coordinating continuous and specific training for all ministry staff. The members of the two AI governance circles will pass on the guidelines and best practice within their organisations. As a result, an AI culture will gradually pervade the entire ministry.

A community of interest, as wide-ranging as possible, should be established for staff wishing to use AI. Sectoral circles are being set up, like the one on big data analytics for maintenance (support organisations, general staff and DGA/DO/SMCO).

2.4.3 Win the skills battle

The recruitment of AI talent is the subject of fierce global competition. Major digital firms are investing in AI R&D centres in France, especially in the Paris region.

What in-house skills do we need?

Artificial intelligence skills are essential in order to remain at the cutting-edge and guide the ministry's choices with regard to the use cases it is interested in. These skills must be retained in house wherever tasks are deemed particularly sensitive.

The skill sets required to carry out projects with an AI component for the armed forces, administrations and support services have been identified. An initial estimate of needs has been made on that basis, subject to consolidation and refinement. Overall, around 80 AI specialists will be needed in 2020, rising to around 200 in 2023, most of them (130) being employed at the DGA.

How do we acquire and retain them?

As these skills are in short supply, it is necessary to target our recruitment and retain skilled staff by keeping them motivated.

As there is currently an AI skills shortage in the private sector, relatively inexperienced engineers are soon offered positions of responsibility with substantial salaries, especially in the Paris region.

The range of defence AI applications and the manipulation of highly specific data may be sources of motivation for recently qualified engineers, who will appreciate the possibilities for carrying out experiments and tests that the ministry can offer them. In addition, they will appreciate being able to enhance their expertise, especially in the context of key partnerships with research organisations. They may also appreciate being associated with major operational issues and having direct contact with actors from the operational sphere, aspects which it is difficult for the civilian sector to offer.

The recruitment of commissioned officers from active or reserve personnel should also be considered in certain cases in order to fill up the pool of experts.

Given the prospect of unprecedented growth in AI occupations, we need to adapt our career paths and take an occupation-based approach at two complementary levels: a group of experts at the cutting-edge of technology, and specialists with dual skills in each of the occupations affected.

AI is rich in techniques and applications. It is essential to monitor developments in the field, covering technologies, projects, products and innovative uses.

2.5 INNOVATION, RESEARCH AND DEVELOPMENT STRATEGY

An eminently dual-use technology, artificial intelligence can make progress within the ministry only through close interaction with the civilian sector, both industrial and academic. Steering this interaction must help both to stimulate innovation and research in specific areas and to capture developments that can be implemented in the systems used by the armed forces, administrations and support services.

2.5.1 Preferential academic partnerships consistent with the national strategy

The Armed Forces Ministry's R&D strategy is aligned with the research strand of government strategy, run by the National Research Agency (ANR).

The ministry will also draw on:

- basic research organisations like INRIA and CNRS;
- engineering schools;
- sectoral players capable of dealing with the issues specific to each system.

Another advantage of this approach will be to promote interest in defence issues among the future AI specialists trained in these institutions.

➢ Set up key partnerships with the main academic research organisations that have significant AI skills.

2.5.2 Direct research towards critical systems

The Armed Forces Ministry's AI uses have features and requirements that are not necessarily the same as those of the uses developed to date for the commercial sector.

These differences highlight real technical challenges that are still far from being resolved. Though undeniable progress has been made in recent years, much still remains to be done to go beyond applications that merely automate elementary or highly specialised tasks, such as operating a robot vacuum cleaner or playing go.

In many ways, these challenges are similar to those that all critical systems using AI will face, whether autonomous vehicles or energy distribution systems. The Armed Forces Ministry will endeavour to guide and support academic and industrial research in AI for critical systems.

➢ Guide academic research and industrial studies as a priority towards the technical challenges to be met for the integration of AI into critical systems.

Example: Drone navigation in an urban environment

In 2018, the ministry financed four CEA/LIST projects offering a quick-win response to use cases it had put forward. CEA/LIST is an AI centre of excellence with over 200 specialist researchers. The CEA model of using spin¬-offs to leverage the value of research applies fully to AI, since more than 20 start-ups with their origins in its research labs have been created over the last five years (Diota, Tridimeo, Sybot, etc.). Reconnaissance drones are being increasingly widely used by armies around the world, partly because they are relatively discreet but above all because they reduce the risk to military personnel. Navigation and mapping in open spaces are relatively simple problems, but navigation below the level of buildings in dense urban environments poses non-trivial obstacle-detection problems, while mapping presents many algorithmic challenges. The project will focus on location and relocation based on vision, real-time 3D reconstruction with obstacle segmentation and time-deferred fine 3D reconstruction, detection and tracking of mobile objects of interest (vehicles, pedestrians) and semantic segmentation in monocular mode. The following is an illustration of a deep learning-based algorithm for the detection and real-time 3D location of vehicles in monocular mode using Deep Manta technology.

2.5.3 Fast-rising investment

The Armed Forces Ministry will invest massively in studies and research in order to prepare future AI applications over the next ten years. Nearly €430 million will be devoted to upstream AI-related studies over the period of the current Military Planning Act (2019-2025). The focus will be partly on stimulating and capturing dual-use innovation and partly on funding defence-specific applications.

The investment is intended to meet the armed forces' immediate short-term needs while also preparing the long-term future. In order to do so, the ministry can draw on a range of resources to support innovation developed by the DGA over a number of years, such as academic theses, the ASTRID and RAPID schemes and ANR-DGA challenges , in addition to its traditional core activity of leading R&T and weapons programmes. The recently created Defence Innovation Agency is intended to enhance the range of options and foster more efficient and agile implementation.

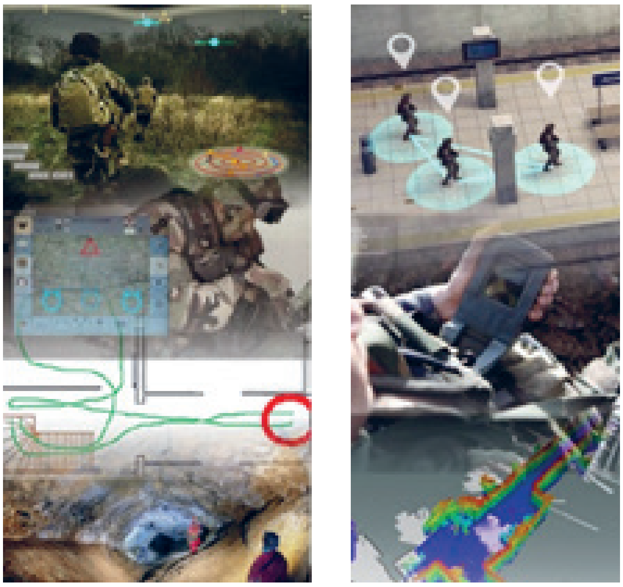
Example: the MALIN (indoor localisation) and DEFALS (falsification detection) challenges

MALIN is a three-year technical competition jointly organised and financed by the DGA and the National Research Agency. Focusing on indoor localisation with the aim of identifying geolocation solutions without a GPS signal in harsh environments, it was launched in December 2017. The six teams taking part, comprising manufacturers and academic research labs, regularly face off in tests of increasing difficulty. The aim is to encourage progress by precisely measuring their performance and identifying their strengths and weaknesses. Different sensor technologies (stereo vision, lidar, inertial units, magnetometers, etc.) are used in systems which are tested under real conditions. The system's effectiveness and robustness depend on *the processing and analysis of the signals collected. Data fusion and AI techniques are decisive: in support of the technologies, AI methods can, for example, analyse an infantryman's steps during his movement and hence optimise reconstruction of his path.*

The DEFALS challenge, now in progress, follows the same principle of emulation. It aims to:

- *Iinitiate and advance image analysis research for the purposes of verifying integrity (blind detection of changes in real images);*
- *mobilise information-processing communities and foster closer links between different disciplines. Corpuses comprise views of natural indoor and outdoor scenes, urban scenes, landscapes, etc*

The development of reliable, automated tools would dispel doubt about information that could be harmful to an individual, a company or an organisation (e.g. retouched press images, industrial hoax) or create a false event (e.g. data enrichment for propaganda purposes).



Illustrations du challenge MALIN

2.5.4 Evaluation and benchmarking for informed investment

In order to inform its R&D investment choices, the ministry will systematically evaluate the results of the studies and research it finances. That evaluation will be both qualitative and quantitative, using metrics specific to systems which contain AI. The ministry will draw on the skills of the National Metrology and Testing Laboratory to design, develop and implement these metrics and the associated test sets. It will also promote this model in an interministerial framework.

2.5.5 Industrial upscaling

In order to bring systems containing AI up to an industrial scale, the Armed Forces Ministry will pursue its innovation strategy and its acquisition strategy in close coherence, under the oversight of the CCIAD.

> ➢ Implement and steer mechanisms between research contracts and the acquisition of solutions in order to facilitate industrial upscaling..

Implementing a defence AI R&D strategy implies raising the level of maturity on the subject among defence contractors. The major defence manufacturers and integrators must be encouraged to think about the use of AI in their systems so that they can rapidly integrate AI-based modules (including those developed by third parties) and develop skills in specifically military uses such as processing for military sensors (radar, sonar, e-warfare, etc.).

2.6 INTERNATIONAL COOPERATION AND EXPORT STRATEGY

AI is a priority area of international cooperation because of its dual-use nature and the possibility of open access to a large number of algorithms and large amounts of data. Cooperation on military uses may take several forms depending on the political goals pursued, the maturity of the technological building-blocks, the project's sensitivity to ethical criteria and the proportion of AI in the cooperation programme as a whole (mere increment or structural building-block).

In order to choose possible cooperations with discernment, it is necessary to clearly identify the goal pursued, especially the use case (which will necessarily be limited), then ascertain the restrictions that will apply either immediately or in the medium term.

2.6.1 Cooperations with various strategic goals

Although the 2017 Defence and National Security Strategic Review recalled that "[...] expertise in artificial intelligence is set to become a sovereignty issue [...]" , that does not rule out the possibility of developing close cooperations, especially within Europe. These may take different forms depending on the goals pursued.

Political goals: structural or occasional cooperation

Our AI cooperation may be set in a European framework, which is the only relevant framework for truly generating powerful synergies, as proposed by the EU's AI strategy. Germany and the UK are key partners in this regard.

Outside Europe, other major countries would like to emancipate themselves from the stranglehold on AI exerted by China and the United States. There may be a convergence of interest on this point, especially if cooperations are established in other areas.

Industrial and technological goals: complementarity or consolidation

Another goal of cooperation may be to gain an industrial or technological advantage. Two cases can be distinguished here:

- **Complementarity:** in this case, cooperation may strengthen our national position by alleviating a partial or total deficiency. Complementarity may be sought at a structural level, through industrial or research policy, or in a targeted way, through projects in a specific segment of AI. It may take the form of industrial alliances or partnerships between research centres.

- **Consolidation** of a comparative advantage: here, the aim of cooperation is to capitalise on an advantage shared by several countries in order to leverage it or achieve critical mass, for example by pooling research resources or sufficient amounts of data, or by creating a large-scale AI integrator. This type of cooperation should be preferred in a European context.

Military performance goals: an essential criterion for the Armed Forces Ministry

Partnerships should not be considered solely from an industrial or capacity standpoint. Interoperability among forces is a key success factor for operational engagements in coalition. This is essential for France, a lead nation which acts as a driver or primary contributor. AI-related military cooperation may aim not only to design and pool AI-enhanced military equipment but also to span other areas such as logistics, simulation, training, organisation and intelligence-sharing. In all events, these cooperation links may be developed in different types of format, whether ad hoc bilateral frameworks or existing formats such as PESCO .

The issue of classified data will arise whatever the nature of the potential partnership, meaning that prior consideration must be given to the question of how such data are shared, depending on the sensitivity of the area of cooperation and the depth of the political link maintained.

➢ At European level, ensure the visibility of our defence position and continue discussions with our partners in cooperation with the General Secretariat for European Affairs (SGAE) and the Ministry for Europe and Foreign Affairs (MEAE).

The seven priority areas of focus lend themselves to cooperation to varying extents. The issues identified to date which pose no problem in terms of maintaining or developing skills or sharing classified data are the following:

- decision and planning support: systems for the conduct of operations at strategic level and for planning, especially logistics (with predictive maintenance);

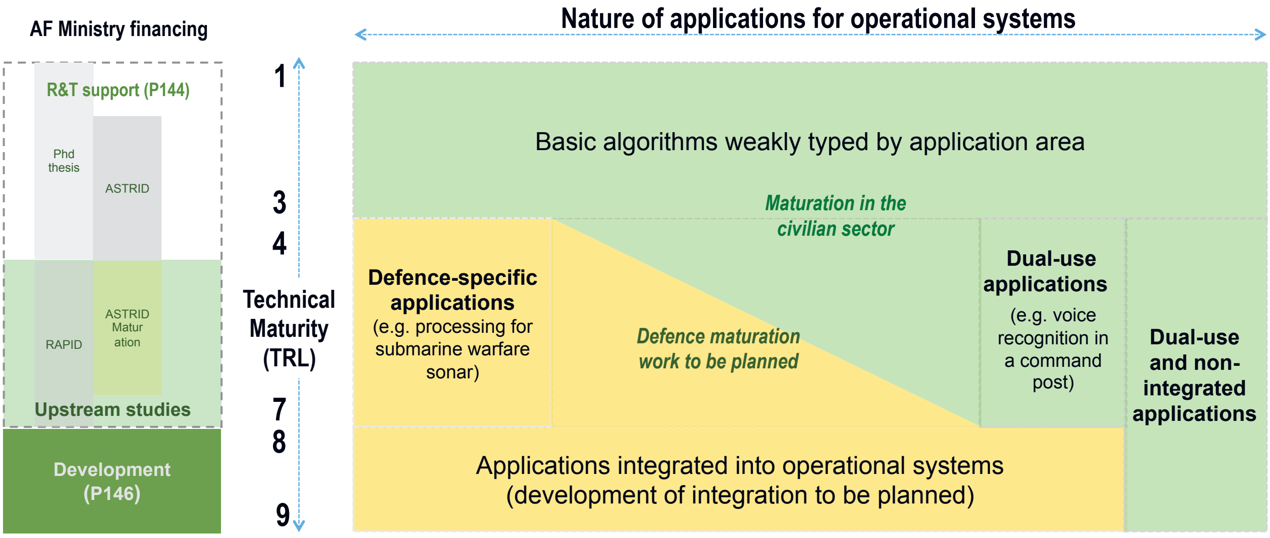

AF Ministry financing
R&T support (P144)
Phd thesis
ASTRID
RAPID
ASTRID Maturation
Upstream studies
Development (P146)
1
3
4
Technical Maturity (TRL)
7
8
9
Nature of applications for operational systems
Basic algorithms weakly typed by application area
Maturation in the civilian sector
Defence-specific applications (e.g. processing for submarine warfare sonar)
Defence maturation work to be planned
Dual-use applications (e.g. voice recognition in a command post)
Dual-use and non-integrated applications
Applications integrated into operational systems (development of integration to be planned)

Figure 5 – Breakdown of investment in AI according to dual-use capability and technical maturity

- collaborative combat: human-machine interfaces, augmented training;

- logistics and operational readiness: mission performance and assisted maintenance applications, especially for cooperation with countries that have the same systems as us;

- intelligence: tools for data mining and synthesis;

- robotics and autonomy: evolved robotic behaviour modules (excluding combat robots and drones and those carrying highly sensitive specialised sensors).

Cooperation is more easily feasible for cross-cutting and support applications, especially in relation to the medicine of the future.

2.6.2 Different circles of potential cooperation

Three circles of possible cooperation can be envisaged on the basis of the criteria described above. They may evolve in a dynamic way, given that the broader context is far from being settled.

First circle: structural partnerships

The first circle comprises our major European partners, with whom cooperation in AI is already an integral part of a mature and fully developed bilateral relationship structured by major programmes. Cooperation here therefore responds to a set of multi-dimensional goals which may be political (greater strategic autonomy, deeper ties), industrial (achievement of critical size in various segments or enhancement of different assets) or military (cooperation relating to capabilities, doctrine and governance).

In addition to these frontline partner countries, NATO, and ACT in particular, provide a privileged framework for cooperation.

Second circle: scoping partners

The second circle comprises the United States, Australia and India, which, though not European, are already partners. Their approach to AI is similar to ours and our cooperation with them could well extend to defence AI. As the leading power in AI, the United States has expressed the wish to cooperate with its key allies, including France, while Australia and India have entered into long-term commitments (Barracuda submarines, acquisition of Rafale fighters). All these projects will incorporate significant AI technological building-blocks, both in the design phase and on the occasion of future retrofits.

Third circle: occasional partners

The third circle comprises countries with which opportunities for targeted cooperation may arise. They include European or non-European partners with genuine AI capabilities or affinities, such as Canada, Japan, Singapore and South Korea. This cooperation may cover all fields, from capabilities and doctrine to intelligence-sharing, training and ethical issues, and may provide a starting-point for closer AI partnerships.

However, this three-circle model does not reflect a solely bilateral vision of our AI cooperation. On the contrary, cross-partnerships between several actors can fertilise such cooperation and may take place between European partners or with our priority partners in the Indo-Pacific zone.

CONCLUSION

In conclusion, the main guidelines for action by the Armed Forces Ministry in the sphere of artificial intelligence are as follows:

- the creation of a ministerial committee that will adjudicate, in particular but not exclusively, on the ethical issues that future AI applications in the military sphere could raise;

- the development and maintenance of a pool of experts within the ministry;

- the framing of a ministry data policy which must guarantee optimum exploitation of data while respecting security and compliance requirements;

- a robust capability roadmap for the responsible and controlled integration of AI both within our armed forces and in the ministry as a whole, respecting the values that our country defends all over the world;

- the introduction of a governance system for the ministry's action in relation to AI, with the creation of a Defence Artificial Intelligence Coordination Unit (CCIAD) within the Defence Innovation Agency;

- the establishment of strategic partnerships with the actors of innovation and cutting-edge research in the field of AI;

- the introduction of mechanisms between research contracts and the acquisition of solutions in order to facilitate industrial upscaling;

- the development of international cooperation, especially at European level, in order to promote our strategic positions and influence the framing of technical standards or regulations on the export of AI-based technologies.

The direction imparted in this way will enable the Armed Forces Ministry to take advantage of the technological revolution now under way without disavowing the values and foundations of its action, whether in operations or in its day-to-day work.

GLOSSARY

ACRONYM	DEFINITION	CONTEXT
3IA	Institut interdisciplinaire d'intelligence artificielle Interdisciplinary artificial intelligence institute	FR
ACT	Allied Command TransformationW	NATO
ADS	Armées, directions et services Armed forces, administrations and support services	MINARM
AFNOR	Association française de normalisation French standardisation association	FR
AI	Artificial Intelligence	
AID	Agence d'innovation de la défense Defence Innovation Agency	MINARM
ANSSI	Agence nationale de la sécurité des systèmes d'information National Information Systems Security Agency	FR
API	Application Programming Interface	TECH
ARTEMIS	Architecture de traitement et d'exploitation massive de l'information multi-sources Architecture for the processing and massive exploitation of multi-source information	DGA
ASIC	Application-Specific Integrated Circuit	TECH
ASTRID	Accompagnement spécifique des travaux de recherche et d'innovation défense Specific support for defence research projects and innovation	DGA
BATX	Baidu, Alibaba, Tencent and Xiaomi	China
BF	Basse fréquence Low frequency	TECH
BITD	Base industrielle et technologique de défense Defence industrial and technological base (DITB)	DGA
C2	Command and Control	MILI
C4ISR	Command, Control, Computers, Communications, Intelligence, Surveillance, Reconnaissance	MILI
CALID	Centre d'analyse de lutte informatique défensive Defensive cyber warfare analysis centre	EMA
CCAC	Convention sur certaines armes classiques Convention on Certain Conventional Weapons	UN
CCIAD	Cellule de coordination de l'intelligence artificielle de défense Defence Artificial Intelligence Coordination Unit	MINARM
CEA	Commissariat à l'énergie atomique Atomic Energy Commission	FR
CEMA	Chef d'état-major des armées Chief of the Defence Staff	EMA
CEN	European Committee for Standardisation	UE
CICDE	Centre interarmées de concepts, de doctrines et d'expérimentations Joint Centre for Concept Development, Doctrine and Experimentation	EMA
CIFRE	Convention industrielle de formation par la recherche Industrial agreements for training through research	FR
CNRS	Centre national de la recherche scientifique National Centre for Scientific Research	FR
CPU	Central Processing Unit	TECH
CSO	Collaborative Support Office	NATO
CSP	Coopération structurée permanente Permanent structured cooperation (PESCO)	EU
CUDA	Compute Unified Device Architecture	TECH
CuDNN	CUDA Deep Neural Network	TECH
DGA	Direction générale pour l'armement Defence Procurement Agency	DGA
DGNUM	Direction générale du numérique et des systèmes d'information et de communication Directorate General for Digital Technology and Information and Communication Systems	MINARM
DGRIS	Direction générale des relations internationales et de la stratégie Directorate General for International Relations and Strategy	MINARM

ACRONYM	DEFINITION	CONTEXT
DIA	Data sciences et intelligence artificielle Data sciences and artificial intelligence	DGA
DIH	Droit international humanitaire International humanitarian law (IHL)	Intl
DIRISI	Direction interarmées des réseaux d'infrastructure et des systèmes d'information Joint Directorate for Infrastructure Networks and Information Systems	EMA
DORESE	Doctrine, organisation, ressources humaines, équipements, soutien, entraînement Doctrine, organisation, human resources, equipment, support and training	MINARM
DRI	Detection, reconnaissance, identification	MILI
DRM	Direction du renseignement militaire Military Intelligence Directorate	EMA
DSP	Digital Signal Processor	TECH
EMA	État-major des armées Defence Staff	EMA
ETI	Entreprise de taille intermédiaire Medium-sized company	FR
FIA	Foreign Intelligence Surveillance Act	US
FPGA	Field Programmable Gate Array	TECH
FREMM	Frégate multi-missions Multi-purpose frigate	SEA
FTI	Frégate de taille intermédiaire Medium-sized frigate	SEA
GAFA	Google, Apple, Facebook and Amazon	US
GE	Guerre électronique Electronic warfare (EW)	MILI
GGE	Groupe d'experts gouvernementaux Group of Government Experts	UN
GIEC	Groupe d'experts intergouvernemental sur l'évolution du climat Intergovernmental Panel on Climate Change (IPCC)	UN
GPS	Global positioning system	
GPU	Graphics Processing Unit	TECH
GT	Groupe de travail Working group	FR
GTB	Gestion technique de bâtiment Building management system	FR
GTIA	Groupement tactique interarmes Battlegroup	LAND
HF	Haute fréquence High frequency	TECH
HLEG	High-level expert group	UE
I2R	Ingénierie de l'informatique et robotique Computer and robotics engineering	DGA
IA	Intelligence Artificielle Artificial intelligence (AI)	TECH
IEC	International Electrotechnical Commission	Intl
IHM	Interface homme-machine Human-machine interface	TECH
INRIA	Institut national de recherche en informatique et automatique National Institute for Research in Computer Science and Automation	FR
IOT	Internet Of Things	TECH
IR	Infra-rouge Infra-red	TECH
ISO	International Standards Organisation	Intl
ITAR	International Traffic in Arms Regulations	US

ACRONYM	DEFINITION	CONTEXT
JAIC	Joint Artificial Intelligence Center	US
LIST	Laboratoire d'intégration de systèmes et des technologies Laboratory for Integration of Systems and Technologies	FR
LPM	Loi de programmation militaire Military Planning Act	MINARM
MALE	Medium Altitude Long Endurance	AIR
MGCS	Main Ground Combat System	LAND
MI	Maîtrise de l'information Information literacy	DGA
MMT	Man-Machine Teaming	AIR
MOD	Ministry of Defence	UK
MRTT	Multi-Role Tanker Transport	AIR
MUST	Méthodologie d'exploitation des données d'Usages des véhicules et d'identification de nouveaux Services pour les usagers et les Territoires	DGA
NAM	Non-Aligned Movement	Intl
OIV	Opérateur d'Importance Vitale Operator of vital importance	FR
ONERA	Office national d'études et de recherches aérospatiales French Aerospace Research Centre	FR
NATO	Organisation du traité de l'Atlantique Nord North Atlantic Treaty Organisation	NATO
PIA	Programme d'investissements d'avenir Investments for the future programme	FR
PME	Petite ou Moyenne Entreprise Small or medium-sized enterprise (SME)	FR
POCEAD	Plateforme d'ouverture, de centralisation, d'exposition et d'analyse des données Data opening, centralisation, exposure and analysis platform	DGA
RAPID	Régime d'appui à l'innovation duale Dual-use innovation support regime	DGA
RENS	Renseignement Intelligence	MILI
RETEX	Retour d'expérience Feedback	MILI
RF	Radio Frequency	TECH
RGPD	Règlement général sur la protection des données General Data Protection Regulation (GDPR)	Intl
RH	Ressources humaines Human resources	FR
ROEM	Renseignement d'origine électromagnétique Signals intelligence (SIGINT)	MILI
ROIM	Renseignement d'origine image Imagery intelligence (IMINT)	MILI
SALA	Système d'armes létales autonome Lethal autonomous weapons system (LAWS)	MILI
SAR	Specific Absorption Rate	TECH
SCORPION	Synergie du contact renforcée par la polyvalence et l'info valorisation	DGA
SGA	Secrétariat général pour l'administration General Secretariat for Administration	MINARM
SMCO	Service du maintien en condition opérationnelle Operational readiness department	DGA
TRL	Technical Readiness Level	TECH
UE	Union Européenne European Union (EU)	UE