MINISTÈRE
DES ARMÉES
Liberté
Égalité
Fraternité

DEFENCE ETHICS COMMITTEE

OPINION ON THE USE OF ARTIFICIAL INTELLIGENCE TECHNOLOGIES BY THE FRENCH ARMED FORCES

14 January 2025

Executive Summary

(1) **Artificial intelligence (AI) is a discipline based in particular on mathematics**, **with the aim of using machines to simulate the mental faculties of human beings.** It consists of various techniques based on modelling knowledge and use of data.

(2) **Spectacular progress made over the last decade, particularly in deep learning, as well as the dramatic rise in data volumes and the development of large language models and generative artificial intelligence, have increased the use of artificial intelligence** in industry, banking, transport, energy, trade, research, healthcare and, more generally, in society and our everyday lives. Artificial intelligence technologies have also been developed to increase surveillance and security resources and, in authoritarian political regimes, means of controlling and repressing the population.

(3) **The issues and interests at stake are such that artificial intelligence has become a global arena of scientific and economic competition involving both governments and businesses**.

(4) **France, as a major global power** with an ecosystem of talented engineers, leading businesses, and a competitive, largely decarbonised national electric power supply, **has adopted a "*National Strategy for AI*" to ensure it remains at the forefront and becomes a pioneer in artificial intelligence**.

(5) This national strategy has been rolled out in three phases in order to secure financial resources, attract talent, and ensure that our country has the necessary infrastructure[1]:

- 2018: the President of the Republic launched the first phase, "*AI for humanity*".
- 2022: the strategy was reinforced, within the framework of the "France 2030" investment plan, to further expand the use of AI and the pool of AI-trained talent.
- 2023: an additional component, dedicated to generative artificial intelligence, was defined to support and accelerate the development of our national champions.

(6) At the same time, and **as military powers worldwide, including our allies but also hostile nations and non-state players, are pursuing programmes aimed at leveraging artificial intelligence technologies to gain operational superiority, the French Republic could not, on any account, exclude the French armed forces from the research and development that will help to safeguard our sovereignty and independence, and meet our international commitments.**

(7) Thus, the **French Strategy for Artificial Intelligence in Defence was initiated in 2019[2] and then further developed in an instruction issued by the Ministry for the Armed Forces on 18 January 2024, defining the "*Ministerial Strategy for Artificial Intelligence*" to be implemented in all the services, directorates and departments of the French Ministry for the Armed Forces.** This strategy, which aims to accelerate the use of artificial intelligence in defence, was unveiled on 8 March 2024 by the Minister for the Armed Forces, Sébastien Lecornu. On 1 May 2024, the Ministerial Agency for Artificial Intelligence in Defence (AMIAD) was established to guarantee **sovereign control over artificial intelligence technologies by the Ministry for the Armed Forces**.

[1] French Ministry for Higher Education and Research website, La stratégie française en intelligence artificielle, https://www.enseignementsup-recherche.gouv.fr/fr/la-strategie-francaise-en-intelligence-artificielle-49166

[2] Speech by the Minister in Saclay, 5 April 2019 and September 2019 report from the French AI Task Force: Artificial intelligence in support of defence.

******

This is the context in which the Ministry for the Armed Forces asked the Defence Ethics Committee for an opinion on artificial intelligence and defence.

This opinion on **the use of artificial intelligence technologies by the French armed forces** identifies **nine principles** and sets out **twelve guidelines**.

Guiding principles identified by the Committee

Principle no. 1: France will only use armed force in compliance with international law to ensure its legitimate defence in the event of aggression, to provide assistance to another European Union Member State in accordance with Article 42-7 of the EU Treaty, to assist one of its allies in accordance with Article 5 of the North Atlantic Treaty, in the context of implementing a United Nations (UN) Security Council resolution or with the consent of the host State. To do so, it must have the means to defend its population, its territory and its interests, to meet its treaty assistance commitments and to take action against hostile state or non-state forces, in all fields and in all environments.

Principle no. 2: Defence is the primary duty of the State, which has the monopoly on the legitimate use of force, but the whole Nation must contribute to it. While the armed forces of the Republic are at the service of the Nation and their mission is to defend the Homeland, citizens, companies and civil society organisations are not "consumers of security" but must play an active part in national defence and security.

Principle no. 3: There can be no "just war" without a just cause and just means. Neither self-defence nor a United Nations (UN) Security Council resolution can justify breaching the rules of the law of armed conflict, and respect for those rules is one of the fundamental values of the Republic.

Principle no. 4: Operations conducted by the armed forces, the use of armed force by such forces and the weapons they employ are exclusively governed by the rules of international humanitarian law (IHL) laid down by the international treaties to which France has adhered whenever they are conducted in a situation of armed conflict, and by the Constitution of the Republic, and the laws and decrees enacted by the French Parliament and Government. Artificial intelligence technologies used in or for military operations are subject to the same legal framework.

Principle no. 5: Research into artificial intelligence systems intended for offensive and defensive use must be conducted in a fully responsible manner. This research must be guided by ethical reflection, in particular regarding the scope and possible developments of its results.

Principle no. 6: The development and deployment of artificial intelligence technologies in military medicine must adhere to the ethical rules specific to the medical field and health research. These technologies must not undermine the decision-making autonomy of healthcare personnel to ensure the highest standard of quality and safety of care.

Principle no. 7: Systems incorporating artificial intelligence technologies must be associated with clearly defined use cases, for which they have been tested, verified and approved, or even certified. These verifications must be reviewed in accordance with changes to the systems and their applications, at a frequency appropriate to the stakes involved.

Principle no. 8: While input provided by artificial intelligence technologies may be useful or even necessary, human decision-making in the use of systems incorporating such technologies must be based

on the context, depending on whether or not the environment is hostile or permissive, and must remain subordinate to the assessment of the situation, which falls under the responsibility of command at the strategic, operational, or tactical level.

Principle no. 9: If subsidiarity is to prevail to ensure that human decisions are made at the appropriate level of situational assessment and at the right time, these decisions must be reported to the higher authority.

Committee's Guidelines

Guideline no. 1: Appropriate methods for verifying legality must be applied, considering the new risks that may arise from the use of certain artificial intelligence technologies in weapons, weapons systems and military operations.

Guideline no. 2: Systems incorporating artificial intelligence technologies must be assessed and qualified at the appropriate level, with requirements proportionate to the expected benefits and the risks to be avoided.

Guideline no. 3: It is essential to ensure that the training and testing of artificial intelligence models intended for the armed forces are based on data that is controlled and, as far as possible, aligned with their military use and the desired level of sovereignty. However, we must safeguard interoperability with our allies to the fullest extent possible. Maintaining control and sovereignty over data will demand an investment and its cost must be accepted.

Guideline no. 4: In general, the training that will be needed to implement systems incorporating artificial intelligence technologies should also raise awareness of information system security risks.

Guideline no. 5: Ergonomic studies should be conducted taking into account the real conditions in which systems incorporating artificial intelligence technologies are used in the context of operations, including in degraded conditions.

Guideline no. 6: As the criteria for accepting automaticity are dictated by the circumstances, artificial intelligence technologies should, where appropriate, enable the level of automation of certain functions to be adjusted based on the assessment made by command and its delegates.

Guideline no. 7: Military training must foster an understanding of transparency documents and, more importantly, develop the ability to recognise when an AI-powered function is degraded, compromised, or insufficient and therefore requires human intervention.

Guideline no. 8: Military personnel must continue to be trained in the fundamentals and expertise of their roles to ensure that they can operate or engage in combat in degraded conditions or without artificial intelligence technologies.

Guideline no. 9: It is essential to define clear chains of responsibility for command, control and execution regardless of the functions performed by a system incorporating artificial intelligence technologies.

Guideline no. 10: Human responsibilities, including those of industrial manufacturers, annotators, programmers, users, supervisors, decision-makers, etc., must be clearly defined to ensure accountability in the use of force.

Guideline no. 11: Operators should be made aware of the importance of providing feedback on the use of artificial intelligence systems.

Guideline no. 12: Studies should be conducted on the long-term impact of artificial intelligence technologies on organisations and human relationships.

TABLE OF CONTENTS

Preamble

(8) The Defence Ethics Committee has been asked by the French Minister for the Armed Forces to give an opinion on "artificial intelligence in defence".

(9) To conduct its work, the Committee interviewed leading civilian and military figures and visited units and organisations involved in the development and use of artificial intelligence technologies.

(10) **Artificial intelligence (AI) is a discipline based in particular on mathematics** with the aim of using machines to simulate the mental faculties of human beings. It consists of various techniques based on modelling knowledge and use of data.

a. This is the essence of the definition given in the Official Journal of the French Republic (JORF) issued on 9 December 2018 (text 58): "***A theoretical and practical interdisciplinary field focused on understanding cognitive and reasoning mechanisms and replicating them through hardware and software systems to assist or replace human activities.***"

b. It is equally the essence of the definition given, six years later, in Article 3(1) of Regulation (EU) 2024/1689 of 13 June 2024, known as the "AI Act"[3].

(11) **Spectacular progress made over the last decade, particularly in deep learning, as well as the dramatic rise in data volumes and the development of large language models and generative artificial intelligence, have increased the use of artificial intelligence** in industry, banking, transport, energy, trade, research, healthcare and, more generally, in society and our everyday lives. Artificial intelligence technologies have also been developed to increase surveillance and security resources and, in authoritarian political regimes, means of controlling and repressing the population.

It is evident that **artificial intelligence and its applications are inherently dual in nature**. It is an innovation that, like others before it, holds great promise for humanity while also raising concerns about employment, social relations, rights and freedoms, as well as global peace and stability.

The issues and interests are stake are such that **artificial intelligence has become a global arena of scientific and economic competition involving both governments and businesses**.

(12) **France, as a major global power** with an ecosystem of talented engineers, leading businesses, and a competitive, largely decarbonised national electric power supply, **has adopted a "*National Strategy for AI*" to ensure it remains at the forefront and becomes a pioneer in artificial intelligence**.

(13) This national strategy has been rolled out in three phases in order to secure financial resources, attract talent, and ensure that our country has the necessary infrastructure[4]:

- 2018: the President of the Republic launched the first phase, "*AI for humanity*".
- 2022: the strategy was reinforced, within the framework of the "France 2030" investment plan, to further expand the use of AI and the pool of AI-trained talent.
- 2023: an additional component, dedicated to generative artificial intelligence, was defined to support and accelerate the development of our national champions.

[3] European Union website, Regulation (EU) 2024/1689. https://eur-lex.europa.eu/eli/reg/2024/1689/oj/eng
[4] French Ministry for Higher Education and Research website, La stratégie française en intelligence artificielle, https://www.enseignementsup-recherche.gouv.fr/fr/la-strategie-francaise-en-intelligence-artificielle-49166

(14) At the same time, and **as military powers worldwide, including our allies but also hostile nations and non-state players, are pursuing programmes aimed at leveraging artificial intelligence technologies to gain operational superiority, the French Republic could not, on any account, exclude the French armed forces from the research and development that will help to safeguard our sovereignty and independence, and meet our international commitments.**

(15) Thus, the **French Strategy for Artificial Intelligence in Defence was initiated in 2019[5] and then further developed in an instruction issued by the Ministry for the Armed Forces on 18 January 2024, defining the *"Ministerial Strategy for Artificial Intelligence"* to be implemented in all the services, directorates and departments of the French Ministry for the Armed Forces.** This strategy, which aims to accelerate the use of artificial intelligence in defence, was unveiled on 8 March 2024 by the Minister for the Armed Forces, Sébastien Lecornu[6]. On 1 May 2024, the Ministerial Agency for Artificial Intelligence in Defence (AMIAD) was established to guarantee **sovereign control over artificial intelligence technologies by the Ministry for the Armed Forces**.

******

This is the context in which the Ministry for the Armed Forces asked the Defence Ethics Committee for an opinion on artificial intelligence and defence.

This opinion follows on from the Committee's opinions given on the integration of autonomy into lethal weapons systems on 29 April 2021 and on the digital environment of combatants on 13 April 2022.

This opinion is given based on the current state of knowledge in artificial intelligence technologies.

******

[5] Speech by the Minister in Saclay, 5 April 2019 (https://www.vie-publique.fr/discours/271295-florence-parly-5042019-intelligence-artificielle-et-defense) and September 2019 report from the French AI Task Force: Artificial intelligence in support of defence.

[6] Speech by the Minister in Palaiseau, 8 March 2024 (https://www.vie-publique.fr/discours/293389-sebastien-lecornu-08032024-intelligence-artificielle)

I. Defence serves the Republic and its values

(16) France **aspires to peace and does not threaten anyone.** The French Constitution also stipulates: *"The French Republic, faithful to its traditions, shall respect the rules of public international law. It shall undertake no war aimed at conquest, nor shall it ever employ force against the freedom of any people.*[7]*"*

(17) **France, which sets great store by multilateralism and an international order based on law, and as a founding member of the United Nations and a permanent member of its Security Council, will only use force on the territory of another State in strict compliance with international law**:

- with the consent of the State in which the intervention takes place;
- on the basis of a Security Council resolution, under Chapter VII of the United Nations Charter: action with respect to threats to the peace, breaches of the peace and acts of aggression[8];
- in the context of individual or collective self-defence in the event of armed aggression within the meaning of Article 51 of the United Nations Charter.

(18) **However, wanting peace is not enough to be at peace**. Terrorism remains a serious threat. Proliferant states continue to defy the international order guaranteed by weakened treaties. Finally, world peace, as well as our independence and security are threatened by the overt or covert actions of hostile or even uninhibited military powers or non-state groups, even on our own continent. These threats could take on a new dimension with the use of artificial intelligence technologies.

(19) **Ensuring our defence and thereby contributing to global stability are absolute imperatives**.

> ***Principle no. 1*: France will only use armed force in compliance with international law to ensure its legitimate defence in the event of aggression, to provide assistance to another European Union Member State in accordance with Article 42-7 of the EU Treaty, to assist one of its allies in accordance with Article 5 of the North Atlantic Treaty, in the context of implementing a United Nations (UN) Security Council resolution or with the consent of the host State. To do so, it must have the means to defend its population, its territory and its interests, to meet its treaty assistance commitments and to take action against hostile state or non-state forces, in all fields and in all environments.**

(20) **Defence plays a key role in safeguarding the fundamental interests of the Nation**, which include national independence, territorial integrity and public protection. These are **constitutional obligations incumbent upon all public authorities, and primarily on the government, as well as on all citizens and all public and private stakeholders.**

> ***Principle no. 2*: Defence is the primary duty of the State, which has the monopoly on the legitimate use of force, but the whole Nation must contribute to it. While the armed forces of the Republic are at the service of the Nation and their mission is to defend the Homeland, citizens, companies and civil society organisations are not "consumers of security" but must play an active part in national defence and security.**

(21) **Defence is an imperative obligation, but not all means of defence are admissible under the laws of the Republic or under international law.**

[7] Preamble to the Constitution of 27 October 1946 maintained in force by the Constitution of 4 October 1958.
[8] For example, intervention in cases of genocide, war crimes, ethnic cleansing and crimes against humanity.

(22) **Firstly, France has ratified most international treaties applicable in the event of armed conflict, as well as those prohibiting or restricting the manufacture, possession and use of certain weapons,** i.e. rules of international law which, for humanitarian reasons, aim to limit the effects of armed conflict or to ensure the protection of victims of armed conflict. These treaties fully commit the State, the public authorities and the French armed forces. **Some of the rules or prohibitions they contain also correspond to principles or values inherent in the ethical corpus of the French armed forces** (*cf.* the opinion of the Defence Ethics Committee on "Ethics in military training").

(23) **Secondly, French criminal law has transposed certain treaty obligations into domestic law, by specifically punishing crimes against humanity[9] as well as war crimes and offences committed during international and non-international armed conflicts,** particularly against persons protected by international law, war crimes and offences related to the conduct of hostilities, and the use of prohibited means or methods of combat[10].

(24) **Lastly, the legislator has enacted the general statute of the military which imposes exceptional duties upon members of the armed forces, including the ultimate sacrifice in the name of defending the Nation, while subjecting their action in combat to strict ethical imperatives and compliance with the law of armed conflict.** The Ministry for the Armed Forces has notably issued the "**Manual on the law of military operations**" setting out the main rules governing the use of force by the French armed forces on national and foreign territory, both in peacetime and during conflict.

***Principle no. 3*: There can be no 'just war' without a just cause and just means. Neither self-defence nor a United Nations (UN) Security Council resolution can justify breaching the rules of the law of armed conflict, and respect for those rules is one of the fundamental values of the Republic.**

II. Artificial intelligence technologies already play a role in our defence and are set to become increasingly important in the future

(25) **By virtue of our Constitution and the principles derived from it, our military operations, the weapons used by our armed forces, and the use of armed force in situations of armed conflict (whether international or otherwise) are governed exclusively by the rules of international humanitarian law (IHL) and by the laws and decrees enacted by the French Parliament and Government.**

(26) **This framework applies to all military engagements of the French armed forces, i.e. the Army, Navy, Air and Space Force, Gendarmerie nationale and their associated formations**.

(27) **Artificial intelligence technologies used in or for military operations are subject to the same legal framework**.

(28) It is worth noting that **Regulation (EU) of 13 June 2024 known as the "AI Act" rightly excludes military AI systems from its scope** (the Regulation defines these systems as *"AI systems placed on the market, put into service, or used with or without modification of such systems for military, defence or national security purposes"* (cf. §24 and Article 2)), **this exclusion being explicitly justified by the**

[9] Articles 211-1 to 213-4-1 of the French Penal Code.
[10] Articles 461-1 to 461-31 and 462-1 to 462-11 of the French Penal Code.

exclusive competence of Member States in these two areas, pursuant to Article 4(2) of the Treaty on European Union and the primacy of public international law.

> ***Principle no. 4*: Operations conducted by the armed forces, the use of armed force by such forces and the weapons they employ are exclusively governed by the rules of international humanitarian law laid down by the international treaties to which France has adhered whenever they are conducted in a situation of armed conflict, and by the Constitution of the Republic, and the laws and decrees enacted by the French Parliament and Government. Artificial intelligence technologies used in or for military operations are subject to the same legal framework.**

(29) Military applications of artificial intelligence technologies can be disruptive factors **in the different areas and environments of conflict and serve as operational assets for those who have control over them.**

(30) As emphasised in the September 2019 report from the AI Task Force "***Artificial intelligence in support of defence***"[11], AI technologies offer potential to enhance operational superiority by:

- **Enhancing situational understanding, anticipation and planning, and enabling faster decision-making**. AI technologies shorten the 'OODA decision loop' (Observe-Orient-Decide-Act) and the 'DCPD intelligence loop' (Direction-Collection-Processing-Dissemination), via a faster and more comprehensive analysis of situations than human processing, by cross-analysing a vast amount of data;
- **Improving soldier protection and training**. AI technologies enhance the effectiveness of weapons systems, improve soldier training and support, and contribute to preserving their health;
- **Promoting compliance with international humanitarian law (IHL) through a better understanding of the operational environment at tactical, operational and strategic levels**. Artificial intelligence technologies enhance the distinction between combatants and non-combatants, improve proportionality by regulating weapon effects based on the threat, and ensure actions are guided by strict necessity;
- **Relieving personnel of time-consuming or repetitive tasks**;
- **Managing increasingly large and complex flows of information**. Artificial intelligence technologies optimise flows and resource management through advanced computing solutions.

(31) **Potential use cases for the armed forces span a wide range of activities with artificial intelligence systems, whether or not integrated into platforms and weapons,** that can contribute to:

a. Operational readiness support (including training and practice);

> For example, the *IA FPN* system, presented by AMIAD at EuroSatory 2024, designed to maximise the success of pilot training. Given the high demands, duration and significant costs of training flight crews, this system aims to alert instructors sufficiently early and focus efforts on overcoming the difficulties encountered by student pilots. By analysing data collected during training, whether in flight or simulation, it therefore increases their chances of success.

b. Intelligence support;

> For example, a system that uses satellite or aerial reconnaissance images to pre-select objects of interest for analysts, but also combines this image data with textual data on the operational situation, to provide intelligence commanders with situation summaries.

[11] AI Task Force Report, www.defense.gouv.fr/sites/default/files/aid/Report of the AI Task Force September 2019.pdf

c. Surveillance and security support, or even surveillance;

   For example, the *Oreille d'or* system, presented by AMIAD at EuroSatory 2024, which processes and sorts vast amounts of acoustic data to highlight relevant signals, allowing operators to apply their professional expertise to the most important information.

d. Planning decision support, or even planning decision-making;

   For example, during an observation phase, systems processing a large amount of data gathered over an extended period to help dispel the fog of war (suspicious activity, presence of elements detected, presence of civilians) and determine the key point of the manoeuvre to be carried out. In the orientation phase, these systems would enhance situational understanding and analysis in a complex, evolving operational environment by leveraging both previously and currently collected data.

   Another example would be a system that assists in selecting an operational plan by simulating a series of events, where different options are tested against enemy modes of actions.

e. Targeting support, or even targeting;

   For example, real-time operational data processing capabilities to enhance the reliability of collateral damage assessments and improve the accuracy and/or choice of weaponry for the intervention.

f. Combat decision support, or even combat decision-making (situational assessment, manoeuvre or firing guidance, etc.);

   For example, the DeMAIA system, presented by AMIAD at EuroSatory 2024, supporting crews during lookout on Griffon vehicles. Due to the challenge crews face in using the images from the six cameras transmitted to the cockpit, the DeMAIA system can detect equipment or personnel up to a distance of three kilometres from the sensors, even on the edge of a forest. For the operators, a red rectangle highlights the detected elements, which they can monitor in real-time.

g. Collaborative combat management support or even collaborative combat management / robotics on land, in the air, at sea, in space (including UAVs, swarms);

   For example, programmes that collect and process a large amount of data from vehicles (land, air and/or sea) to propose trajectories through hostile environments that maximise chances of survival, solutions for countering threats, allocating tasks, etc.

h. Cybersecurity support;

   For example, systems that optimise the processes of defensive computer warfare, automated fault-finding or mass data processing, to enhance the effectiveness and responsiveness of information and weapons systems in the event of an incident.

i. Information warfare support;

   For example, a system for detecting deepfakes and false information targeting the armed forces (presented by AMIAD at EuroSatory 2024). Given the capability of artificial intelligence systems to generate false information, and the serious consequences of its dissemination through social media or the internet, this system supports operators by identifying manipulated video, image or audio content, aiding in operational responses (such as denunciation).

j. Strengthening support (in-service support (ISS), combatant support, etc.);

   For example, the Resistance system (presented by AMIAD at EuroSatory 2024) that offers instant translation of foreign languages on smartphones, enabling communication with civilian populations and local authorities during operations, even offline and without

a network. This solution meets the recurring need for translation, especially when a human translator is unavailable.

Another example is the Rora system for the rapid identification of spare parts (presented by AMIAD at EuroSatory 2024). When faced with parts that are difficult to identify, this application can accurately recognise a part from a simple photograph, saving maintenance operators time and reducing the risk of delays in maintenance and supply.

k. Design and drafting support (weapons systems, staff documents, etc.);

For example, systems that query the data available within headquarters to generate thematic summary reports for users.

(32) **Having regard for the strategic and operational stakes involved, research into artificial intelligence systems intended for offensive and defensive use must be conducted in a fully responsible manner in order to maintain or enhance the capabilities of our armed forces. This research must be guided by ethical reflection, in particular regarding the scope and possible developments of its results.**

(33) The purpose and scope of research programmes must remain open without stipulating any prohibitions. To protect our forces, we need to know what systems an enemy could employ even if, for ethical reasons, they could not be used by our own forces.

***Principle no. 5*: Research into artificial intelligence systems intended for offensive and defensive use must be conducted in a fully responsible manner. This research must be guided by ethical reflection, in particular regarding the scope and possible developments of its results.**

***Principle no. 6*: The development and deployment of artificial intelligence technologies in military medicine must adhere to the ethical rules specific to the medical field and health research. These technologies must not undermine the decision-making autonomy of healthcare personnel to ensure the highest standard of quality and safety of care.**

(34) If artificial intelligence technologies were to be used to augment combatants, it would be necessary, in line with the Ministry's doctrine in this area, to uphold the principle of human dignity, ensure that the proposed interventions are harmless, and preserve the physical and mental health of military personnel[12].

(35) The national and European legal frameworks are, prima facie, in favour of the development of artificial intelligence technologies for military use, including when these technologies are initially designed and developed for civilian purposes and later adapted for use by the armed forces. However, it will be necessary to assess **the long-term impact on European industry and research** of a regulation which, like the EU Regulation of 13 June 2024, comprises 257 pages, including 89 pages of general considerations and definitions, 113 articles and 13 normative annexes. **The risk is that European research and industry could ultimately fall behind, leaving the French armed forces and European defence with only one option:** "***AI developed by others***".

(36) It will also be important to assess the potential impacts of using so-called "organic" artificial intelligence technologies (in areas such as human resources, finance and logistics) to enable some of this data to be pooled and processed in support of operations.

[12] Cf. Opinion of the Defence Ethics Committee of 18 September 2020 on 'the augmented soldier'.

(37) Attention should therefore be paid to the risks of incorporating civilian standards or rules into organic artificial intelligence programmes as this could create barriers to operations.

(38) A review of the potential use cases highlights issues of legality and accountability (designer, command, operator) and raises questions about dependability (uncertainties, errors and failures), and disinhibition (by distancing combatants from the field).

III. Effective management of military uses of artificial intelligence is both essential and possible

(39) **It is important to remember that military artificial intelligence technologies encompass a much broader scope than autonomous weapons systems (AWS) with which they should not be confused. Therefore, military applications of artificial intelligence technologies must be accompanied by all the necessary specific guarantees, particularly in terms of legality, design, implementation and long-term considerations.**

A. Verifying legality

(40) **An artificial intelligence technology is not a weapon in itself. Therefore, it cannot be classified as an unlawful weapon that could be prohibited by an international treaty**.

(41) **However, certain uses of artificial intelligence technologies for military purposes, and the conditions under which they are employed, may, in some cases, be considered combat methods and resources whose effects cannot be limited, and are therefore prohibited by the law of armed conflict.** Recent conflicts on Europe's Eastern flank and in the Middle East have highlighted both the operational advantages and the risks associated with using equipment that incorporates artificial intelligence technologies in armed conflict.

(42) The question thus arises regarding the compliance of certain systems incorporating artificial intelligence technologies with international humanitarian law, pursuant to Article 36 of the Protocol Additional to the Geneva Conventions of 12 August 1949 and relating to the protection of victims of international armed conflict of 8 June 1977 (PA I). According to that provision: "*In the study, development, acquisition or adoption of a new weapon, means or method of warfare, a High Contracting Party is under an obligation to determine whether its employment would, in some or all circumstances, be prohibited by this Protocol or by any other rule of international law applicable to the High Contracting Party*".[13]

(43) In line with its commitments, France has established procedures for reviewing legality and integrating an analysis of compliance with international law at each stage in defence procurement. In particular, the Committee emphasises that this review is conducted, as required, at each stage in a weapons system's life cycle, including preparation, production, and operational use. During the operational phase, which is often the longest, a legality review is conducted whenever "obsolescence or integration of innovations into the weapon, means or doctrine contribute to changing the functions in a manner that could challenge the previous legality opinion".[14]

[13] Committee's opinion of 6 January 2021 on integrating autonomy into lethal weapons systems §126
[14] Committee's opinion of 6 January 2021 on integrating autonomy into lethal weapons systems §128

(44) Given the risks mentioned above, the Committee underlines the importance and relevance of conducting a full legality review whenever an artificial intelligence technology is developed or integrated into a system used by the armed forces, particularly for functions such as identification, classification or opening fire.

(45) Therefore, in accordance with ministerial procedures, it is essential to apply methods tailored to the new risks that may arise from the use of certain artificial intelligence technologies in weapons, weapons systems and military operations.

(46) It will then be for the responsible authorities to decide on the deployment and use of such technologies in compliance with the ethical approach outlined here.

***Guideline no. 1*: Appropriate methods for verifying legality must be applied, considering the new risks that may arise from the use of certain artificial intelligence technologies in weapons, weapons systems and military operations.**

B. Guarantees during design

a. Dependability of artificial intelligence technologies and qualification in line with the risks inherent in their use.

(47) Dependability requires the applications of artificial intelligence technologies to be associated with defined use cases, for which the technologies have been tested and verified. A dependability review is also based on the following criteria:

- **Compliance:** the compliance of an artificial intelligence technology means that the results produced by the system integrating the technology align with the objective for which it was designed. The results in turn correspond to the system's specifications which must meet the needs of users.

- **Transparency**: a system integrating artificial intelligence technologies must be transparent at the relevant levels. This means providing factual elements that enable the various stakeholders (designer, user authority, end user, etc.) to understand how and why a specific result was obtained. In this context, these stakeholders should be provided with documentation outlining the purpose of the artificial intelligence technologies used, the methods and reasoning behind the results, the training and testing data employed, responsibilities in design and implementation, and an assessment of the consequences of the use of the system.

  The importance for the armed forces of having transparency criteria goes beyond simply having information that validates the qualification of a weapons system. Such criteria would also support military training, provide answers to questions from commanders or operators regarding the artificial intelligence technologies used, and enable the armed forces to justify their use of a specific artificial intelligence technology to the political authorities.

- **Robustness**: this requirement reflects the extent to which the artificial intelligence system performs its intended function reliably and precisely, particularly in the face of unforeseen events (such as an adverse attack, wrong use), the introduction of data that differs to the data used to train the system or in the event of a failure (does the system switch to degraded mode? Does it recover its capabilities?).

***Principle no. 7*: Systems incorporating artificial intelligence technologies must be associated with clearly defined use cases, for which they have been tested, verified and approved, or even certified. These verifications must be reviewed in accordance with changes to the systems and their applications, at a frequency appropriate to the stakes involved.**

***Guideline no. 2*: Systems incorporating artificial intelligence technologies must be assessed and qualified at the appropriate level, with requirements proportionate to the expected benefits and the risks to be avoided.**

b. Data sovereignty for machine-learning technologies

(48) Over and above the conditions of use, some tools must provide the commander or combatant with very reliable results. Therefore, in these particular cases, the training and testing of artificial intelligence models intended for the armed forces must be based on data that is controlled and, as far as possible, aligned with their military use and the desired level of sovereignty. However, we must safeguard interoperability with our allies to the fullest extent possible. Maintaining control and sovereignty over data will demand an investment and its cost must be accepted.

***Guideline no. 3*: It is essential to ensure that the training and testing of artificial intelligence models intended for the armed forces are based on data that is controlled and, as far as possible, aligned with their military use and the desired level of sovereignty. However, we must safeguard interoperability with our allies to the fullest extent possible. Maintaining control and sovereignty over data will demand an investment and its cost must be accepted.**

c. Managing the cybersecurity risks of systems incorporating artificial intelligence technologies

(49) Non-compliance and risks relating to the performance of systems incorporating artificial intelligence technologies are not the only risks associated with their use. Additionally, before or during the use of these systems, there are risks of compromising:

- data integrity, by deliberate or unintended pollution, which distorts the results of the learning process;
- data unavailability, which hampers the operation of an artificial intelligence technology that requires comparison with reference data;
- the confidentiality of data and/or results following the theft of sensitive information.

(50) Current technical recommendations include:

- selecting technologies adapted to each use case;
- using countermeasures (such as tattoos, cryptography, specific training of models, etc.) and appropriate defences.

***Guideline no. 4*: In general, the training that will be needed to implement systems incorporating artificial intelligence technologies should also raise awareness of information system security risks.**

d. Ergonomic studies and human control

(51) The question of man-machine interfaces is extremely important. Therefore, the Committee reiterates the guideline provided in its opinion on the digital environment of combatants, according to which human factors require special attention. This guideline is valid for numerous applications and means that ergonomic studies should be conducted based on the real conditions faced by combatants in operations.

(52) Analysing and defining the necessary and sufficient level of human control, without restricting the capabilities of the system incorporating artificial intelligence technologies (at the risk of losing the benefits), is a complex issue that must take various factors into account. These factors include human aspects (such as fatigue, stress, skill, etc.), technical aspects (transparency, validation support, etc.) and contextual elements (dynamics and complexity of the environment).

(53) This analysis should be based on an appropriate context and doctrine of use supported by advanced experimentation and evaluation to ensure that systems incorporating artificial intelligence technologies fulfill a relevant role while guaranteeing sufficient and adequate human oversight.

***Guideline no. 5*: Ergonomic studies should be conducted taking into account the real conditions in which systems incorporating artificial intelligence technologies are used in the context of operations, including in degraded conditions.**

C. Controlled implementation

e. The role of personnel must be maintained in the decision-making process

(54) The Committee notes that the current conflicts in Ukraine and the Near East are theatres in which artificial intelligence systems are employed in large-scale and unrestrained combat. These conflicts illustrate the rapid evolution in the manner of conducting military operations.

(55) While the purpose of an artificial intelligence system is to provide information for decision-making, evaluation of the risks and the decision to accept or refuse them must remain human prerogatives.

(56) In armed conflict, the operational environment and intensity of combat constantly influence the level of automaticity and delegation decided by command. The extent to which an artificial intelligence system is used and assigned decision-making or other specific tasks must therefore be determined based on a full assessment of the weapons system environment and the operational context.

***Principle no. 8*: While input provided by artificial intelligence technologies may be useful or even necessary, human decision-making in the use of systems incorporating such technologies must be based on the context, depending on whether or not the environment is hostile or permissive, and must remain subordinate to the assessment of the situation, which falls under the responsibility of command at the strategic, operational or tactical level.**

***Principle no. 9*: If subsidiarity is to prevail to ensure that human decisions are made at the appropriate level of situational assessment and at the right time, these decisions must be reported to the higher authority.**

(57) When deploying artificial intelligence technologies for decision support at tactical, operational and strategic levels, special attention must be paid to the interaction between the decision support tool and the military commander. In high-pressure scenarios in which decisions must be taken fast, the tool must

be sufficiently robust to proposed reliable "instinctive solutions" when the decision-maker experiences cognitive overload.

(58) Therefore, particularly in complex and/or time-sensitive situations, such as saturation attacks, enemy deployment of automated systems, or more broadly, high-intensity combat, it must be possible to automate certain tasks using artificial intelligence technologies to maintain the necessary responsiveness and operational scale.

***Guideline no. 6*: As the criteria for accepting automaticity are dictated by the circumstances, artificial intelligence technologies should, where appropriate, enable the level of automation of certain functions to be adjusted based on the assessment made by command and its delegates.**

f. Commander and combatant training

(59) Soldiers must be trained for a type of combat that is compliant with our values.

(60) The use of artificial intelligence technologies and military training in such uses must not, on any account, affect the ability of military personnel to apply the fundamental principles of their roles which underpin the added-value of human assessment.

(61) To ensure that doctrine on the use of force is fully applied to artificial intelligence systems, it will be necessary to train operators in the limits of these systems.

(62) Military commanders will need a more comprehensive acculturation process to ensure that artificial intelligence systems do not become black boxes for them and that they use such systems with a full understanding of their benefits and limits.

(63) Training must aim to enable judgement and prevent misuse due to over-reliance on the results generated by artificial intelligence systems.

***Guideline no. 7*: Military training must foster an understanding of transparency documents and, more importantly, develop the ability to recognise when an AI-powered function is degraded, compromised, or insufficient and therefore requires human intervention.**

***Guideline no. 8*: Military personnel must continue to be trained in the fundamentals and expertise of their roles to ensure that they can operate or engage in combat in degraded conditions or without artificial intelligence technologies.**

g. Responsibility throughout the life cycle and use (including design, training, decision-making, use) of systems incorporating artificial intelligence technologies.

(64) Responsibility cannot be attributed to an artificial intelligence system.

(65) Human responsibility in the design, deployment and use of artificial intelligence technologies is an inalienable principle. The highest values of our civilisation and our constitutional order require human responsibility in all circumstances.

***Guideline no. 9*: It is essential to define clear chains of responsibility for command, control and execution regardless of the functions performed by a system incorporating artificial intelligence technologies.**

***Guideline no. 10*: Human responsibilities, including those of industrial manufacturers, annotators, programmers, users, supervisors, decision-makers, etc., must be clearly defined to ensure accountability in the use of force.**

h. Dialectics of judgment

(66) The principle of preserving human involvement in decision-making processes means accepting to compare the results generated by systems incorporating artificial intelligence technologies with human reasoning and behaviour.

(67) Therefore, military operators or commanders must have the ability to exercise their own judgment, drawing on their own situational assessment, experience, intuition, or dialogue with their teams or staff, and must retain the right to make a decision that differs from the result produced by the system incorporating artificial intelligence technologies.

(68) Doubts about the results generated by systems incorporating artificial intelligence technologies, stemming from the fact that it conflicts with the intuition and deductive reasoning of a military operator or commander, must be recognised as legitimate.

(69) If a commander has doubts, their ethic should prompt them to make the necessary verifications whenever possible.

D. Long-term guarantees

i. Feedback

(70) It is important to identify and characterise errors encountered when testing or using a system incorporating artificial intelligence technologies (including identifying the context of use, the type of error, etc.).

Guideline no. 11: Operators should be made aware of the importance of providing feedback on the use of artificial intelligence systems.

j. Retraining systems incorporating artificial intelligence technologies

(71) The ability to retrain and correct systems incorporating artificial intelligence technologies with real data annotated according to their compliance with our values is crucial. This ability will become all the more essential as advancements in research and technology enhance the reliability of artificial intelligence technologies.

k. Impact of artificial intelligence technologies on organisations and human relationships

***Guideline no. 12*: Studies should be conducted on the long-term impact of artificial intelligence technologies on organisations and human relationships.**

APPENDIX

DEFENCE ETHICS COMMITTEE

The Defence Ethics Committee was established on 10 January 2020 by the French Minister for the Armed Forces. It is tasked with **issuing opinions and recommendations to inform political and military authorities of the ethical issues raised by changes in the military function, changes in conflicts, and scientific and technological innovations in defence**. It comprises **18 qualified persons** nominated by the Minister. They are appointed for three years, and may be re-appointed once.

Current Composition (since March 2023)

Bernard PECHEUR	Defence Ethics Committee Chair, Section President (h), *Conseil d'État*
Bernard THORETTE	Defence Ethics Committee Vice-Chair, Army General (2S), former Army Chief of Staff (CEMAT).
Christine BALAGUÉ	Professor at *Institut Mines-Telecom / IMT-BS*, holder of the Good in Tech Chair
Serge BARCELLINI	President of *Le Souvenir Français*.
Marie-Germaine BOUSSER	Professor emeritus of neurology, member of the *Académie nationale de médecine*.
Walter BRUYERE-OSTELLS	University Professor, member of the Scientific Council for Historical Research in Defence.
Patrick CAREIL	Inspector-General of Finance (h).
Hervé de COURREGES	Army Major General. Director of IHEDN (Institute of higher studies in national defence), in charge of higher military education.
Michel GOSTIAUX	Chief Defence Procurement Engineer
Xavier LANDOT	Rear-Admiral (2S).
Aurélie LECAM	Commissioner for the Armed Forces.
Kévin LIMONIER	Senior lecturer, deputy director of GEODE research centre.
Ariane MICHAUD	Chief Medical Officer of the Armed Forces.
Bruno PAUPY	French Air and Space Force Colonel.
Guillaume SCHLUMBERGER	Senior State Administrator.
Catherine TESSIER	Director of Research and research integrity and research ethics officer at the French national aerospace research centre (ONERA).
Nicolas THERY	President of the *Crédit Mutuel* foundations.
Cathy THILLY-SOUSSAN	Financial, legal and ethics advisor, *Direction Générale de l'Armement* (DGA)

Previous Composition (2020-2023)

Bernard PECHEUR	Defence Ethics Committee Chair, Section President (h), *Conseil d'État.*
Henri BENTEGEAT	Defence Ethics Committee Vice-Chair, Army General (2S), former Chief of Defence Staff (CEMA).
Christine BALAGUÉ	Professor at IMT-BS, holder of the Good in Tech Chair.
Rose-Marie ANTOINE	Former President of the *Office national des anciens combattants et victimes de guerre*.
Marie-Germaine BOUSSER	Professor emeritus of neurology, member of the *Académie nationale de médecine*.
Frédérick DOUZET	Professor at the French Institute of Geopolitics (Paris VIII University), director of GEODE research centre.
Hervé DREVILLON	Director of Research, SHD.
Michel GOSTIAUX	Chief Defence Procurement Engineer.
Laurent HERMANN	Rear-Admiral.
Jean-Baptiste JEANGENE-VILMER	French philosopher, jurist and political scientist.
Aurélie LECAM	Commissioner for the Armed Forces, legal advisor.
Bruno PAUPY	French Air and Space Force Colonel.
Philippe ROUANET DE BERCHOUX	Chief Medical Officer of the Armed Forces.
Guillaume SCHLUMBERGER	General Controller of the Armed Forces on extraordinary mission.
Catherine TESSIER	Director of Research and research integrity and research ethics officer at the French national aerospace research centre (ONERA).
Nicolas THERY	President of the *Confédération Nationale du Crédit Mutuel*.
Cathy THILLY-SOUSSAN	Financial, legal and ethics advisor, *Direction Générale de l'Armement* (DGA).
Bernard THORETTE	Army General (2S), former Army Chief of Staff (CEMAT).

Committee Opinions

The opinions of the Defence Ethics Committee and their translations are available on the website[15]:

2020: Augmented Soldier
2021: Integration of Autonomy into Lethal Weapons Systems
2022: Digital Environment of Combatants
2022: Ethics in Military Training.
2022: Ethics of Space Defence
2024: The Role of Civil Actors in a Comprehensive Defence Strategy

[15] https://www.defense.gouv.fr/comite-dethique-defense