



# ARTICLE DU MOIS

Octobre 2025

Sécurité et Défense

## **L'intelligence artificielle de défense : un changement de paradigme stratégique**

Par Elina Ribeiro da Costa

Mots clés : IA, défense, sécurité, cybersécurité, innovation, technologie

## RESUME

Depuis la fin de la Guerre froide, la transformation numérique des forces armées s'est accélérée, l'intelligence artificielle (IA) est désormais un levier stratégique pour la supériorité opérationnelle et la souveraineté nationale. L'« IA de défense » englobe les usages, doctrines et dispositifs mobilisant l'IA dans le secteur militaire, visant à accélérer la décision, protéger les forces et préserver l'autonomie technologique. L'émergence de l'IA militaire s'inscrit aujourd'hui dans un contexte géopolitique compétitif : États-Unis, Chine, Russie et France, entre autres, investissent massivement dans ce secteur pour maintenir leur supériorité technologique. En France, la stratégie « AI for Humanity » et la Task Force IA Défense (2018-2019) ont posé les bases d'une IA souveraine, éthique et opérationnelle. Au niveau européen, le AI Act encadre l'IA civile, tandis que des initiatives comme le SCAF et le Fonds européen de défense soutiennent la coopération militaire en IA.

L'IA se définit comme la capacité des machines à imiter des processus cognitifs humains. Elle repose sur le machine learning et le deep learning, permettant aux systèmes d'apprendre à partir de données pour anticiper, classifier et prédire. Toutefois, la doctrine du human in the loop garantit que la décision finale reste humaine. Dans la défense, l'IA intervient dans de nombreux secteurs comme le renseignement, la planification tactique, la robotique autonome, la logistique et la cybersécurité. Cela a pour conséquence la transformation de la temporalité et de la nature du commandement militaire. Toutefois, ces innovations soulèvent des enjeux éthiques et juridiques notamment liés à la délégation de la décision létale, la neutralité des données, la responsabilité en cas de faute, et la vulnérabilité face aux attaques informatiques. Au-delà de ces questionnements, l'IA fait face à d'importantes limites technologiques comme les hallucinations et la manipulation des données et donc la fragilisation de la formation de l'IA par un acteur humain.

Ainsi, l'IA transforme la guerre et le monde militaire, mais sa mise en œuvre exige un équilibre entre performance, contrôle humain, éthique et respect du droit international.

## TABLE DES MATIERES

### Introduction

1. L'IA : à quoi ça sert et comment ça marche ?
  - 1.1. L'IA et son fonctionnement
  - 1.2. Contexte d'émergence de l'IA
2. Ses usages aujourd'hui dans la défense
  - 2.1. Usages actuels
  - 2.2. Évolutions et améliorations futures
  - 2.3. Multiplicité des acteurs de face à l'IA de défense aujourd'hui
3. Les limites de l'IA
  - 3.1. Limites éthiques
  - 3.2. Limites légales
  - 3.3. Limites technologiques
4. Focus : situation sur la situation en France
  - 4.1. La stratégie ministérielle
  - 4.2. La recherche et l'innovation
  - 4.3. Vers un développement Européen ?

### Conclusion

## INTRODUCTION

Depuis la fin de la Guerre froide, la transformation numérique du champ de bataille s'est accélérée avec la miniaturisation des capteurs, l'explosion des données et l'amélioration des capacités de calcul. Aujourd'hui, l'intelligence artificielle (IA) est considérée comme la phase la plus avancée de cette évolution. Elle s'impose comme un levier stratégique, modifiant la manière de concevoir, de planifier et de conduire la guerre. L'IA est plus qu'un instrument d'aide à la décision : elle peut devenir un acteur déterminant de la supériorité opérationnelle et de la souveraineté nationale.

Le concept d'« IA de défense » recouvre l'ensemble des usages, doctrines, infrastructures et dispositifs mobilisant l'intelligence artificielle au service du secteur militaire d'un État. En France, elle est définie comme un « champ interdisciplinaire théorique et pratique qui a pour objet la compréhension de mécanismes de la cognition et de la réflexion, et leur imitation par un dispositif matériel logiciel, à des fins d'assistance ou de substitution à des activités humaines »<sup>1</sup>.

La recherche militaire contemporaine se structure autour de trois impératifs majeurs : accélérer la décision, protéger les forces et préserver la souveraineté technologique. L'intelligence artificielle répond à ces derniers grâce à une puissance de traitement et de simulation. Mais cela reste toutefois à nuancer en partie à cause de l'accélération de la course technologique entre les grandes puissances, la complexité croissante des systèmes et le risque d'autonomisation des machines au détriment du jugement humain.

L'enjeu de cet article est donc de comprendre comment l'IA s'est imposée dans la défense moderne, quels en sont les usages et les perspectives, mais aussi les limites. Nous verrons également comment la France, au sein d'un environnement stratégique européen et mondial en mutation, tente de développer une IA de défense souveraine, responsable et conforme au droit international.

# 1. L'IA : à quoi ça sert et comment ça marche ?

## 1.1. L'IA et son fonctionnement

L'intelligence artificielle (IA) est aujourd'hui au cœur des enjeux de la société contemporaine. C'est un outil de plus en plus répandu dans de nombreux aspects de la vie. Cette dernière, est difficile à saisir et à définir. Selon l'encyclopédie Larousse, elle serait un « ensemble de théories et de techniques mises en œuvre en vue de réaliser des machines capables de simuler l'intelligence humaine », c'est-à-dire une imitation de l'intelligence humaine, du fonctionnement du cerveau, de la raison et de la réflexion. Cette volonté d'imitation de l'intelligence humaine n'est toutefois pas encore atteinte à cause de son caractère technologique. D'un autre côté, selon le Japan-Singapore AI Center, l'IA se définirait comme un « Ensemble de systèmes qui démontrent des capacités comparables au raisonnement humain pour améliorer la qualité de vie et améliorer la compétitivité économique. ». Cette définition prend en compte les objectifs de l'IA de rechercher l'efficacité et la rentabilité et ainsi soutenir l'humain dans plusieurs domaines pour se substituer à ses défauts (lenteur et incertitude par exemple). Au regard de la multiplicité des définitions et de la difficulté à saisir la réalité de cet objet, il est nécessaire de prendre des précautions particulières quant à son utilisation. Pour autant, la définition qui semble s'imposer en première approche est celle de l'imitation de l'intelligence humaine<sup>2</sup>.

Pour y parvenir, l'IA s'appuie notamment sur le *machine learning*, un ensemble de méthodes dans lequel on fournit des données permettant au système d'apprendre à reconnaître des motifs ou à prédire des résultats. Parmi ces méthodes il est possible de citer les réseaux neuronaux, qui sont inspirés du fonctionnement du cerveau humain et organisés en couches de « neurones » artificiels qui précisent leurs connexions grâce à l'apprentissage. Le *deep learning* est une forme particulière de ces réseaux qui utilise de nombreuses couches de « neurones », cela le rend particulièrement performant pour résoudre des tâches complexes notamment dans les domaines de l'analyse du signal sonore ou visuel.

## 1. L'IA : à quoi ça sert et comment ça marche ?

L'IA se distingue ainsi des programmes informatiques traditionnels, qui suivent des règles fixes et ne peuvent évoluer sans intervention humaine. Il est tout de même important de ne pas oublier que l'IA n'est pas indépendante mais bien soumise à l'intervention humaine qui lui fournit les données et influence donc ses réponses. Dans un premier temps, il faut « entraîner » l'IA pour qu'elle apprenne à classer les données qui lui sont données. Elle pourra ensuite tendre vers une sorte d'autonomie pour classer de nouvelles données elle-même. Toutefois, la doctrine du « human in the loop », qui stipule que la décision finale, notamment en matière d'emploi de la force, doit toujours demeurer sous contrôle humain permet de garder l'IA sous contrôle humain.

L'intégration de l'IA dans la défense répond à un questionnement stratégique qui est de maintenir la supériorité opérationnelle dans un environnement caractérisé par la complexité, la saturation informationnelle et la vitesse d'exécution. Le Ministère des Armées considère que « la maîtrise des technologies d'intelligence artificielle est essentielle à la souveraineté militaire et à la crédibilité de la dissuasion ». Ainsi, l'IA intervient à plusieurs niveaux des opérations militaires :

- Le renseignement et la surveillance, grâce à l'analyse automatisée d'images satellitaires et de signaux électromagnétiques.
- La planification et la décision tactique, par la simulation de scénarios et la prévision comportementale des forces adverses.
- La robotique et les systèmes autonomes, tels que les drones, véhicules ou robots terrestres collaboratifs.
- La logistique et le maintien en condition opérationnelle, où les algorithmes permettent de prévoir les pannes, optimiser les flux et accélérer le soutien des troupes.
- La cybersécurité et la guerre informationnelle, domaines dans lesquels l'IA permet la détection de menaces, la défense adaptative des systèmes et la lutte contre la désinformation<sup>3</sup>.

L'IA remet en question la temporalité de la décision militaire : elle permet de réduire le délai de décision et modifie la structure de commandement. Elle modifie aussi la nature du renseignement militaire car au lieu de collecter et d'analyser, les systèmes apprenants anticipent, détectent et hiérarchisent les menaces en temps réel. Le général François Lecointre, ancien chef d'état-major des armées, soulignait que « l'enjeu n'est plus seulement de disposer d'armes plus puissantes, mais d'un commandement plus informé, plus agile et plus réactif »<sup>4</sup>.

# 1. L'IA : à quoi ça sert et comment ça marche ?

## 1.2. Contexte d'émergence de l'IA

L'émergence de l'intelligence artificielle s'inscrit dans une compétition géopolitique entre puissances pour la maîtrise de cette technologie, ce qui a placé l'IA au cœur des rapports de force internationaux. Les premières recherches en IA, dans les années 1950 se concentrent sur la volonté de simuler les processus cognitifs humains à travers des programmes logiques. C'est au XXI<sup>e</sup> siècle que l'IA a intégré les secteurs économiques et militaires. En effet, l'IA moderne arrive très soudainement sur le devant de la scène. Les modèles d'IA générative (capable de créer des contenus tels que du texte, du son, des images) comme ChatGPT créé aux États-Unis par OpenAI, DeepSeek créé par l'entreprise du même nom en Chine ainsi que Mistral en France en sont des exemples flagrants.

Parallèlement, les États-Unis, la Chine, la Russie ainsi que plusieurs autres puissances ont massivement investi dans la recherche militaire en IA. Pour le chercheur François-Bernard Huyghe, l'intelligence artificielle « redéfinit les rapports de force entre nations, en conférant à ceux qui la maîtrisent une capacité d'anticipation, de détection et de frappe accrue ». Les États-Unis, par exemple, ont lancé dès 2018 le Joint Artificial Intelligence Center (JAIC), devenu aujourd'hui Chief Digital and Artificial Intelligence Office. La Chine considère l'IA comme une composante de la guerre intelligente (zhinenghua zhanzheng) pour fusionner automatisation, cyberspace et guerre cognitive<sup>5</sup>. La France a très tôt compris l'importance de ne pas dépendre de solutions étrangères. Dès 2018, le président Emmanuel Macron lançait la stratégie nationale AI for Humanity, puis la Task Force IA Défense en 2019. Le rapport, L'intelligence artificielle au service de la défense fixe trois objectifs :

- Garantir la souveraineté technologique.
- Développer les usages opérationnels.
- Inscire l'IA dans une démarche éthique et juridique<sup>6</sup>.

Au niveau européen, le Règlement sur l'intelligence artificielle (AI Act), adopté en 2024, encadre les usages civils de l'IA, tout en excluant explicitement les applications militaires de son champ d'application, reconnaissant ainsi la compétence exclusive des États membres en matière de défense<sup>7</sup>.

## 2. Ses usages aujourd'hui dans la défense

### 2.1. Usages actuels

L'intelligence artificielle transforme aujourd'hui les modes d'action militaires. Son usage s'étend des fonctions de renseignement et surveillance à la planification des opérations, en passant par la logistique et la cybersécurité. L'IA agit à toutes les étapes des décisions militaires, du recueil de l'information à la conduite des opérations sur le terrain.

L'un des domaines les plus avancés d'application de l'IA est la fusion de données de renseignement. Le ministère des Armées indique que « les algorithmes de reconnaissance visuelle et acoustique permettent d'analyser plus rapidement les images satellitaires, les flux vidéo de drones et les signaux radio, offrant ainsi un avantage opérationnel considérable dans les opérations de renseignement »<sup>8</sup>. Ces outils ont déjà été intégrés dans plusieurs opérations, notamment pour la détection de positions ennemies en environnement urbain, la surveillance maritime ou le contrôle de zones aériennes contestées. L'analyse automatisée d'images permet d'identifier les changements que l'œil humain aurait du mal à remarquer dans le même temps donné.

L'IA contribue aussi à la planification opérationnelle par la simulation de scénarios complexes. Les armées peuvent utiliser des modèles qui servent à estimer les comportements adverses, anticiper les menaces et optimiser le déploiement des forces. Le CICDE, dans son document Commandement et contrôle interarmées en environnement multimilieux et multichamps, le concept exploratoire interarmées CEIA-3.0\_C2IA-M2MC « vision prospective » (2022) expliquait cette place de l'IA dans les armées du futur<sup>9</sup>.

La logistique bénéficie elle aussi de l'IA pour anticiper les besoins et réduire les pannes. L'analyse prédictive permet d'évaluer la durée de vie d'un équipement, d'identifier les risques de défaillance et d'optimiser la gestion des stocks. L'armée de l'air française expérimente ainsi des solutions de maintenance assistée par IA sur ses Rafale et A400M, permettant d'éviter des immobilisations coûteuses. Cette approche augmente la disponibilité des matériels tout en réduisant les coûts d'entretien.

## 2. Ses usages aujourd'hui dans la défense

### 2.2. Évolutions et améliorations futures

Les développements à venir laissent entrevoir une transformation encore plus profonde des armées. L'intelligence artificielle ne se limite plus à l'analyse ou au soutien logistique ; elle s'intègre progressivement aux systèmes d'armes autonomes.

L'une des tendances majeures réside dans l'émergence de systèmes de combat collaboratifs qui permettent aux drones, robots terrestres et véhicules habités d'échanger des informations pour optimiser leurs actions. Le programme français SCAF (Système de combat aérien du futur), mené en coopération avec l'Allemagne et l'Espagne, repose sur une intégration de l'IA afin de coordonner des drones avec un avion de combat de nouvelle génération<sup>11</sup>. Ces innovations reposent sur des capacités de calcul embarqué, des capteurs interconnectés et une autonomie décisionnelle accrue. Le défi majeur consiste à accorder la rapidité d'action de l'algorithme avec le contrôle humain. En effet, plus un système devient autonome, plus il devient complexe à superviser en temps réel<sup>10</sup>.

L'IA transforme aussi la nature même de la guerre. Plusieurs chercheurs évoquent la naissance d'une guerre cognitive, où la maîtrise de l'information et la manipulation des perceptions deviennent cruciales. L'IA joue un rôle central pour détecter les fausses informations et en produire (deepfakes, bots, contenus ciblés)<sup>11</sup>. Les armées s'intéressent également à l'intégration de l'IA dans les systèmes de commandement et de contrôle (C2). L'objectif est d'atteindre une « vitesse de décision supérieure », capable de surpasser celle de l'adversaire dans la boucle OODA. Cette dernière se résume en 4 points centraux afin de favoriser une réponse rapide et une adaptation face aux changements :

- Observer : Collecter des informations sur la situation.
- Orienter : Analyser et interpréter ces informations pour donner du sens à la situation.
- Décider : Déterminer un plan d'action basé sur les informations comprises.
- Agir : Mettre en œuvre le plan d'action.

## 2. Ses usages aujourd'hui dans la défense

La cybersécurité constitue un autre champ d'évolution. L'IA permet de détecter, contrer et anticiper des cyberattaques. En France, le Commandement de la cyberdéfense (ComCyber) développe des solutions d'analyse fondées sur des algorithmes d'apprentissage capables d'identifier une intrusion dissimulée dans des millions de connexions<sup>12</sup>. L'IA permet de dépasser les approches traditionnelles basées uniquement sur des règles statiques ou des indicateurs précis (noms de fichiers, adresses IP, signatures de malware par exemple). Ces méthodes sont efficaces pour détecter des menaces déjà connues mais ne permettent pas de faire face aux nouvelles attaques. De plus, les solutions de détection comportementale qui existent aujourd'hui comme les EDR (*Endpoint Detection & Response*) qui surveillent les actions des processus et identifient des comportements anormaux ne sont pas suffisantes.

Cependant, l'IA permet de combler ces manquements grâce au *machine learning* et au *deep learning*. Elle peut, en effet, identifier de nouveaux schémas et développer ses connaissances sur les nouvelles menaces. Cela lui permet d'améliorer la précision de la détection comportementale mais aussi de prendre des décisions plus rapides (isoler une machine ou bloquer une connexion par exemple). À terme, l'IA devrait permettre d'automatiser partiellement la réponse cyber avec l'identification de la source et le confinement du périmètre. Cette perspective ouvre toutefois un débat éthique et juridique, notamment sur le risque d'escalade non maîtrisée en cas de riposte automatique<sup>13</sup>.

## 2. Ses usages aujourd'hui dans la défense

### 2.3. Multiplicité des acteurs de face à l'IA de défense aujourd'hui

Le développement de l'IA de défense ne relève plus exclusivement des États. Il s'appuie sur un écosystème d'acteurs hybrides qui regroupe industrie, recherche publique et entreprises du numérique. Les grands groupes comme Thales, Safran ou Dassault jouent un rôle essentiel dans le développement d'applications d'IA. Parallèlement, des start-ups contribuent à la R&D. L'Agence de l'innovation de défense (AID) soutient ces initiatives à travers des appels à projets et des programmes de co-développement<sup>14</sup>. Ce mélange public-privé pose toutefois la question de la confidentialité des données et de la dépendance technologique vis-à-vis des acteurs civils. De plus, les plateformes de cloud ou les processeurs utilisés dans les calculs d'IA sont souvent d'origine non européenne, ce qui fragilise la souveraineté numérique. Au niveau international, l'OTAN a adopté en 2021 une stratégie pour l'intelligence artificielle, visant à harmoniser les pratiques de ses membres et à promouvoir une IA « digne de confiance »<sup>15</sup>. Enfin, la coopération européenne, bien qu'encore fragile, se renforce avec des initiatives comme le Fonds européen de défense (FEDef) et le European Defence Innovation Scheme (EDIS), qui financent des projets conjoints en IA.

A cet égard, il est nécessaire de parler de l'explosion de la capitalisation en bourse de Nvidia. La multinationale américaine des puces électroniques Nvidia est devenue le 29 octobre 2025 la première entreprise au monde à franchir les 5 000 milliards de dollars de valorisation boursière. Elle dépasse ainsi Méta, Netflix et Tesla réunies<sup>16</sup>. Son activité se concentre en grande partie sur l'IA, dont elle est l'un des leaders incontestés. Ainsi, elle entretient des partenariats avec des pays comme la Corée du Sud et des entreprises du secteur industriel, ce qui la place au cœur du dynamisme d'innovation mais également économique.

Cet entrecroisement d'acteurs de différents niveaux fait naître de nouveaux partenariats et de nouvelles perspectives pour l'IA de défense. Ainsi, avec la guerre en Ukraine, l'entreprise américaine Palantir et le ministère de la Transformation numérique d'Ukraine ont monté un partenariat permettant à l'Ukraine d'avoir accès aux innovations de l'entreprise américaine et en contrepartie, cette dernière a accès aux données du terrain, souvent peu accessibles pour développer ses technologies<sup>17</sup>.

## 3. Les limites de l'IA

### 3.1. Limites éthiques

Le premier enjeu éthique majeur concerne la délégation du pouvoir de décision à la machine, notamment pour l'emploi de la force. Les systèmes d'armes létales autonomes (SALA) posent la question fondamentale de savoir si une machine peut décider de tuer. Le Comité d'éthique de la défense rappelle que « la responsabilité de l'action militaire, y compris dans un environnement numérisé, doit demeurer humaine »<sup>18</sup>. Cette position s'inscrit dans la doctrine du human in the loop, selon laquelle la décision finale ne doit pas être déléguée à un algorithme. Pourtant, l'instantanéité des combats modernes pousse à réduire la part du jugement humain : dans un contexte où la vitesse d'exécution peut faire la différence, les armées cherchent à automatiser les prises de décision. Cette tension entre efficacité opérationnelle et contrôle éthique constitue un défi central. Par ailleurs, la résolution A/C.1/79/L.77 présentée à l'ONU par l'Autriche et un groupe de 26 États co-auteurs souligne « l'importance du rôle humain dans le recours à la force pour garantir la responsabilité et l'obligation de rendre des comptes, et pour que les États respectent le droit international »<sup>19</sup>. Cette dernière a été votée contre par quelques États, notamment la Russie et la Biélorussie. Cela montre que cette notion est largement admise par de nombreux États, même si elle est mise en cause par quelques exceptions.

L'éthique de l'IA militaire repose aussi sur la qualité et la neutralité des données. Un algorithme entraîné sur des données biaisées peut produire des décisions biaisées elles aussi. Le rapport du Comité d'éthique de la défense insiste sur le danger d'une « illusion de précision » : un algorithme peut sembler plus fiable qu'il ne l'est réellement, ce qui risque de créer une trop grande confiance en la technologie<sup>20</sup>. Les armées doivent donc créer des protocoles d'audit et de validation indépendants des systèmes d'IA avant tout usage opérationnel.

Au-delà de la responsabilité, l'IA questionne la valeur morale du combat. La distance entre le soldat et l'acte de guerre, déjà amorcée avec les frappes de drones, augmente avec l'automatisation des processus de décision. Comme l'écrit Grégoire Chamayou, « plus la guerre devient technologique, plus elle tend à effacer la figure de l'adversaire et la conscience morale de l'acte létal »<sup>21</sup>. Le risque d'une banalisation de la violence est à questionner. C'est pourquoi la doctrine française met l'accent sur la « conservation du lien moral entre le combattant et l'acte de combat », considérée comme essentielle à la légitimité de l'usage de la force<sup>22</sup>.

## 3. Les limites de l'IA

### 3.2. Limités légales

L'IA militaire confronte le droit international humanitaire (DIH) à de nouveaux défis. Les Conventions de Genève reposent sur des principes tels que la distinction entre civils et combattants, la proportionnalité et la responsabilité. Mais ces principes présupposent l'existence d'un agent moral capable de jugement, ce que l'IA n'est pas. L'article 36 du Protocole additionnel I aux Conventions de Genève impose aux États de vérifier la conformité aux lois des nouvelles armes avant leur déploiement<sup>23</sup>. En France, cette obligation se traduit par une évaluation juridique systématique menée par la Direction des affaires juridiques du ministère des Armées. Le Comité d'éthique de la défense recommande d'étendre ce contrôle à tous les systèmes utilisant de l'IA, y compris à des fins non létales<sup>24</sup>.

A cela s'ajoute la difficulté d'attribution de la responsabilité en cas de faute commise par une IA militaire. Si une machine autonome cause des pertes civiles il est difficile de déterminer la personne qui sera tenu pour responsable. La doctrine juridique dominante rejette l'idée d'une « responsabilité de la machine » car seul un acteur humain ou institutionnel peut être responsable de ses actes<sup>25</sup>. Toutefois, les systèmes d'apprentissage fonctionnent comme des « boîtes noires » : il peut être impossible de comprendre les raisons exactes d'une erreur. D'où la nécessité de développer des IA explicables et auditées, pour garantir une traçabilité juridique<sup>26</sup>.

Au niveau national, la France encadre l'usage de l'IA par des dispositifs internes : la Charte de l'éthique de l'intelligence artificielle de défense (2024) fixe des principes de transparence, de supervision humaine et de conformité au droit international humanitaire. Sur le plan international, aucune convention ne régit encore spécifiquement les armes autonomes. Des discussions sont en cours au sein des Nations unies, sous l'égide du Groupe d'experts gouvernementaux sur les systèmes d'armes létales autonomes (GGE-SALA), mais les positions divergent : certains États (États-Unis, Russie, Israël) refusent toute interdiction préventive, tandis que d'autres (France, Allemagne, Autriche) plaident pour un encadrement strict<sup>27</sup>.

## 3. Les limites de l'IA

### 3.3. Limites technologiques

Les systèmes d'IA demeurent vulnérables. Ils peuvent être manipulés par des attaques par exemples contradictoires qui consistent à soumettre des entrées malicieuses ou corrompues au système d'IA en phase de production pour le tromper et fausser sa formation<sup>28</sup>. Une image légèrement altérée peut suffire à induire une erreur de classification. Ces attaques représentent une menace majeure pour la fiabilité des systèmes<sup>29</sup>. Le risque d'une « guerre algorithmique » dans laquelle les adversaires cherchent à corrompre ou dégrader les IA adverses plutôt qu'à détruire leurs infrastructures physiques est parfois mis en avant. Ainsi, la résilience de l'IA devient une dimension importante de la supériorité opérationnelle<sup>30</sup>.

A cela s'ajoute, la complexité des systèmes d'IA qui rend leur intégration difficile dans la chaîne de commandement. Les opérateurs doivent en comprendre les limites pour ne pas tomber dans une dépendance cognitive face à la machine. Comme le rappelle Thierry Berthier pour la Revue Défense Nationale, l'intelligence artificielle ne doit pas devenir une instance d'autorité, mais demeurer un instrument de discernement au service du commandement<sup>31</sup>. Le défi réside donc dans la construction d'une confiance raisonnée : faire de l'IA un outil de performance sans en faire une source d'aliénation décisionnelle.

D'un autre côté, les modèles d'IA, même très avancés peuvent créer des résultats incorrects ou incohérents. On parle alors d'« hallucinations ». Cela se traduit par des analyses fausses ou des classifications inexactes. Bertrand Rondepierre, directeur de l'AMIAD, explique dans le podcast du Collimateur Les mondes de l'IA que les IA militaires ne sont pas évaluées selon les mêmes standards que les IA civiles. Les attentes sur la précision et la robustesse peuvent être moins strictes, ou simplement différentes, selon le contexte opérationnel. Par exemple : une IA civile pour la santé doit quasiment éviter toute erreur pour la sécurité des patients alors qu'une IA militaire peut tolérer un certain niveau d'erreurs si le système global inclut un humain pour vérifier ou corriger les décisions, ou si la rapidité et l'adaptabilité compensent les risques.

## 4. Focus : la situation en France

### 4.1. La stratégie ministérielle

La France a été l'un des premiers pays européens à définir une stratégie d'intelligence artificielle de défense. Dès 2019, la Task Force IA Défense identifiait des priorités de développement. Cette impulsion a conduit à la publication en janvier 2024 d'une Stratégie ministérielle pour l'intelligence artificielle de défense, qui fixe trois objectifs principaux :

- Garantir la souveraineté des technologies critiques (algorithmes, données, processeurs, cloud sécurisé).
- Développer des capacités opérationnelles augmentées.
- Promouvoir une IA de confiance, conforme aux valeurs républicaines et au droit international<sup>32</sup>.

Le ministère des Armées souligne que cette stratégie repose sur une approche globale : elle ne se limite pas à la recherche technologique mais prend également en compte la formation, la doctrine et la culture opérationnelle. Le commandement militaire est encouragé à se familiariser avec les outils numériques afin de maintenir la supériorité du discernement humain<sup>33</sup>. Cette initiative a permis la création, en 2024, de l'Agence ministérielle pour l'intelligence artificielle de défense (AMIAD), en charge de coordonner les programmes de recherche et d'assurer une maîtrise souveraine des technologies<sup>34</sup>. Le rapport du Comité d'éthique de la Défense rappelle que cela s'inscrit dans la continuité de la Stratégie nationale pour l'intelligence artificielle lancée en 2018, prolongée par France 2030 (3,3 Milliard d'euros dédiés à l'IA dans tous secteurs confondus), est renforcée en 2023 avec un volet dédié à l'IA générative<sup>35</sup>. Ces politiques visent à garantir que l'emploi de l'IA dans la défense reste conforme au droit international humanitaire, à la Constitution et aux valeurs républicaines, tout en permettant à la France de demeurer une puissance technologique de premier plan.

Le Comité d'éthique de la défense joue un rôle clé dans ce dispositif : il évalue la conformité des projets à la Charte de l'éthique de l'intelligence artificielle militaire, veille à la conformité aux lois des systèmes et formule des recommandations en matière de responsabilité et de transparence<sup>36</sup>. La doctrine française revendique une intelligence artificielle humanisée, où la puissance technologique est soumise au cadre juridique et moral.

## 4. Focus : la situation en France

### 4.2. La recherche et l'innovation

La recherche constitue le pilier de l'autonomie française en matière d'IA de défense. L'Agence de l'innovation de défense (AID) coordonne la recherche et soutient de nombreux projets d'IA en partenariat avec les laboratoires publics, les PME et les start-ups. Parmi les initiatives phares, on peut citer :

- Le programme Descartes sur la simulation et la modélisation prédictive.
- Les travaux de l'ONERA sur la vision embarquée et la navigation autonome.
- Les projets de l'Inria et de l'Institut Polytechnique de Paris sur l'apprentissage profond et la cybersécurité<sup>37</sup>.

L'armée française investit également dans les technologies émergentes à travers le plan France 2030, avec plusieurs milliards d'euros pour l'intelligence artificielle, la robotique et la quantique. L'objectif est de créer une synergie civilo-militaire en mobilisant les innovations du secteur privé pour renforcer la base industrielle et technologique de défense (BITD). Toutefois, la recherche française fait face à deux défis majeurs :

- La pénurie de talents spécialisés, souvent attirés par les géants du numérique.
- La dépendance technologique aux composants étrangers, notamment pour les semi-conducteurs et les infrastructures de calcul intensif.

Pour pallier ces faiblesses, le gouvernement encourage la constitution de pôles d'excellence régionaux (Toulouse, Saclay, Rennes) et le renforcement des coopérations européennes dans le cadre du Fonds européen de défense.

## 4. Focus : la situation en France

### 4.3. Vers un développement européen ?

La dimension européenne est devenue incontournable. Aucun État membre ne peut, seul, rivaliser avec les investissements américains ou chinois. L'Union européenne cherche donc à structurer une autonomie stratégique autour de l'IA. Le Fonds européen de défense (FEDef) finance des projets collaboratifs en IA appliquée à la défense. Des initiatives comme le Système de combat aérien du futur (SCAF) et le Main Ground Combat System (MGCS) qui serait le futur char européen, intègrent des modules d'intelligence artificielle pour la coordination entre systèmes interconnectés<sup>38</sup>. L'objectif est double : mutualiser les coûts de recherche et garantir l'interopérabilité entre les forces armées européennes.

Parallèlement, la Commission européenne soutient la création d'un écosystème de données sécurisé pour la défense afin de réduire la dépendance aux infrastructures extra-européennes. Malgré tout, des divergences persistent : certains États (France, Allemagne) plaident pour une IA éthique et contrôlée, tandis que d'autres privilégient la rapidité d'innovation au détriment du cadre normatif. Comme le souligne un rapport de l'IRIS, « la réussite du projet européen dépendra de sa capacité à conjuguer autonomie stratégique, mutualisation des moyens et cohérence éthique ». La France, forte de son avance doctrinale, pourrait jouer un rôle moteur dans cette construction d'une IA de défense européenne responsable et souveraine.

## CONCLUSION

L'intelligence artificielle s'impose comme un changement important pour les forces armées contemporaines. Elle transforme la guerre elle-même, la rendant plus rapide, plus complexe, mais aussi plus abstraite. Cependant, cette évolution ne doit pas être réduite à une simple avancée technologique. L'IA met à l'épreuve le droit, la morale et la souveraineté. Il existe des dilemmes éthiques liés à la délégation de la décision et des vulnérabilités inhérentes aux systèmes d'apprentissage. La France, comme de nombreux autres Etats, propose un modèle d'IA militaire éthique, souveraine et responsable. Ce modèle repose sur un équilibre entre innovation et contrôle, entre puissance technologique et primauté de l'humain. Dans un monde où la compétition technologique semble parfois primer, cette approche offre une autre voie. L'enjeu des années à venir sera de maintenir cet équilibre fragile.

## BIBLIOGRAPHIE

<sup>1</sup>Gary, Arnaud. "Intelligence artificielle et armées françaises: une technologie du présent à mettre en œuvre immédiatement." *Revue Défense Nationale - Cahier*, no. 1264 (2022).

<sup>2</sup>Comité d'études de Défense Nationale. (2022). *Revue Défense Nationale*, 2022/10 (n° 855) : « Souveraineté et résilience numérique ». Cahiers Cairn.

<sup>3</sup>Ministère des Armées, « Comprendre l'IA de défense », site officiel, 2024.

<sup>4</sup>Bernard Pecheur (dir.), *Avis sur l'usage des technologies d'intelligence artificielle par les forces armées*, 13-14.

<sup>5</sup>Ministère des Armées, *Task Force IA : L'intelligence artificielle au service de la défense* (Paris, 2019).

<sup>6</sup>Comité d'études de Défense Nationale. (2022). *Revue Défense Nationale*, 2022/10 (n° 855) : « Souveraineté et résilience numérique ». Cahiers Cairn.

<sup>7</sup>Ministère des Armées, « Comprendre l'IA de défense », op. cit.

<sup>8</sup>Comité d'éthique de la défense, *Avis sur l'usage des technologies d'intelligence artificielle par les forces armées* (Paris: Ministère des Armées, 2024), 19.

<sup>9</sup>Ministère des Armées, *Programme SCAF : Vers un système de combat collaboratif*, communiqué officiel, 2024.

<sup>10</sup>Centre interarmées de concepts, de doctrines et d'expérimentations (CICDE). *Concept exploratoire interarmées CEIA-3.0 : C2IA-M2MC - Prospective 2022*. Ministère des Armées, 18 juillet 2022.

<sup>11</sup>Comité d'éthique de la défense, *Avis sur l'usage des technologies d'intelligence artificielle par les forces armées*, 24.

<sup>12</sup>François-Bernard Huyghe, « Les implications stratégiques de l'intelligence artificielle », Cairn.info, 2022.

<sup>13</sup>Vie publique, *Usage des technologies d'intelligence artificielle par les forces armées (rapport public, 2024)*, 29.

## BIBLIOGRAPHIE

<sup>14</sup>Agence nationale de la sécurité des systèmes d'information (ANSSI), L'IA au service de la détection et de la réponse à incident, (ANSSI, 2025)

<sup>15</sup>Agence de l'innovation de défense (AID), Appel à projets Innovation Défense – IA 2024, Paris.

<sup>16</sup>OTAN, Artificial Intelligence Strategy for Defence and Security, Bruxelles, 2021.

<sup>17</sup>Le Monde, "Nvidia, multinationale américaine des puces électroniques, devient la première entreprise à dépasser les 5 000 milliards de dollars de capitalisation boursière," Le Monde, 29 octobre 2025.

<sup>18</sup>Hunder, Max. "Ukraine Sees 'Priceless' Digital Battlefield Data Trove as Key to West's Support." Reuters, August 27, 2025.

<sup>19</sup>Comité d'éthique de la défense, Avis sur l'usage des technologies d'intelligence artificielle par les forces armées, 22.

<sup>20</sup>Jones, Isabelle. "161 States Vote Against the Machine at the UN General Assembly." Stop Killer Robots, 5 November 2024.

<sup>21</sup>Grégoire Chamayou, Théorie du drone (Paris : La Fabrique, 2013), 23.

<sup>22</sup>Ibid, 67.

<sup>23</sup>Comité d'éthique de la défense, Avis sur l'usage des technologies d'intelligence artificielle par les forces armées, 25.

<sup>24</sup>Protocole additionnel I aux Conventions de Genève du 12 août 1949, art. 36, 1977.

<sup>25</sup>Bernard Pecheur (dir.), Avis sur l'usage des technologies d'intelligence artificielle par les forces armées, 28-29.

<sup>26</sup>François-Bernard Huyghe, « Les implications stratégiques de l'intelligence artificielle », Cairn.info, 2022.

## BIBLIOGRAPHIE

<sup>27</sup>Comité d'éthique de la défense, Avis sur l'usage des technologies d'intelligence artificielle par les forces armées, 30.

<sup>28</sup>Nations unies, Groupe d'experts gouvernementaux sur les systèmes d'armes létales autonomes (GGE-SALA), Rapport 2023.

<sup>29</sup>Commission nationale de l'informatique et des libertés, "Attaque par exemples contradictoires (adversarial examples attack)," CNIL, consulté le 20/11/2025.

<sup>30</sup>Vie publique, Usage des technologies d'intelligence artificielle par les forces armées (rapport public, 2024), 41.

<sup>31</sup>Ibid., 42.

<sup>32</sup>Revue Défense Nationale, « Intelligence artificielle, numérique, drones, robots : vers la guerre de demain », Cairn.info, 2022.

<sup>33</sup>Ministère des Armées, Stratégie ministérielle pour l'intelligence artificielle de défense, 5-6.

<sup>34</sup>Ibid., 8.

<sup>35</sup>Comité d'éthique de la défense, Avis sur l'usage des technologies d'intelligence artificielle par les forces armées, 4.

<sup>36</sup>Ibid., 3.

<sup>37</sup>Ibid, 33.

<sup>38</sup>Agence de l'innovation de défense (AID), Rapport annuel 2024, Paris, 12-15.

<sup>39</sup>IRIS, « Quel rôle l'IA est-elle susceptible de jouer dans le futur de la défense ? », Paris : Institut de Relations Internationales et Stratégiques, 2023.