MINISTÈRE
DES ARMÉES
Liberté
Égalité
Fraternité

COMITÉ D'ÉTHIQUE DE LA DÉFENSE

AVIS SUR L'USAGE DES TECHNOLOGIES D'INTELLIGENCE ARTIFICIELLE PAR LES FORCES ARMÉES

14 janvier 2025

Synthèse exécutive

(1) **L'intelligence artificielle (IA) est une discipline fondée notamment sur les** mathématiques **en vue de simuler des facultés mentales humaines avec des machines.** Elle regroupe un ensemble de techniques fondées sur la modélisation de connaissances et sur l'exploitation de données.

(2) **Les progrès spectaculaires réalisés dans la dernière décennie notamment avec l'apprentissage profond, l'explosion du volume des données, le développement de grands modèles de langue et l'essor de l'intelligence artificielle générative, ont permis de multiplier les usages de l'intelligence artificielle** dans l'industrie, la banque, les transports, l'énergie, le commerce, la recherche, la santé et plus généralement dans la société et notre vie quotidienne. Des technologies d'intelligence artificielle ont parallèlement été développées pour accroître les moyens de surveillance et de sécurité mais aussi, dans les régimes politiques autoritaires, les instruments de contrôle et de répression des populations.

(3) **Du fait des enjeux et des intérêts en cause, l'intelligence artificielle est devenue le champ d'une compétition scientifique et économique mondiale mettant aux prises les États comme les entreprises**.

(4) **La France, puissance de premier rang**, qui peut s'appuyer sur un écosystème d'ingénieurs de talent, d'entreprises performantes et qui bénéficie d'une énergie électrique nationale, largement décarbonée et compétitive, **s'est dotée d'une « *Stratégie nationale en intelligence artificielle* » pour éviter tout décrochage et devenir un pays pionnier en matière d'intelligence artificielle**.

(5) Cette stratégie nationale s'est déployée en trois phases en vue de mobiliser les moyens financiers, de faire émerger les talents et de doter notre pays des infrastructures essentielles [1]:

- 2018 : la première phase, « *AI for humanity* », a été lancée par le Président de la République.
- 2022 : la stratégie a été renforcée, dans le cadre de « France 2030 », pour diffuser plus largement les usages de l'IA et former davantage de talents.
- 2023 : un volet complémentaire, consacré à l'intelligence artificielle générative, a été défini afin d'accompagner et d'accélérer le développement de nos champions nationaux.

(6) Parallèlement**,** et **alors que dans le monde des puissances militaires, parmi nos alliés comme parmi des acteurs étatiques et non étatiques qui nous sont hostiles, ont engagé des programmes visant à leur conférer, grâce aux technologies de l'intelligence artificielle, l'ascendant opérationnel, la République ne pouvait, en aucun cas et à aucun prix, tenir les armées françaises à l'écart de recherches et de développements permettant de garantir notre souveraineté, notre indépendance et le respect de nos engagements internationaux.**

(7) À cet effet, la **stratégie française pour l'intelligence artificielle de défense a été engagée en 2019** [2] **puis amplifiée et développée dans une instruction du ministre des armées, en date du 18 janvier 2024, définissant la *« Stratégie ministérielle pour l'intelligence artificielle* » à mettre en œuvre dans l'ensemble des armées, directions et services du ministère des armées.** Cette stratégie, dont l'objectif est d'accélérer l'utilisation d'une intelligence artificielle de défense, a été dévoilée le 8 mars 2024 par

[1] Site du ministère de l'enseignement supérieur et de la recherche, La stratégie française en intelligence artificielle, https://www.enseignementsup-recherche.gouv.fr/fr/la-strategie-francaise-en-intelligence-artificielle-49166

[2] Discours de la Ministre à Saclay le 5 avril 2019 et rapport de la *Task force IA* de septembre 2019 « *l'intelligence artificielle au service de la défense* ».

le ministre des armées, Sébastien Lecornu. Le 1er mai 2024, l'agence ministérielle pour l'intelligence artificielle de défense (AMIAD) a été créée afin d'assurer une **maîtrise souveraine des technologies de l'intelligence artificielle par le ministère des armées**.

******

C'est dans ce contexte que le Comité d'éthique de la défense a été saisi par le ministre des Armées d'une demande d'avis sur l'intelligence artificielle et la défense.

Le présent avis consacré à **l'usage des technologies d'intelligence artificielle par les forces armées** dégage **9 principes** et formule **12 recommandations**.

Les principes directeurs dégagés par le Comité

Principe n°1 : La France n'entend recourir à la force des armes que dans le respect de la légalité internationale pour assurer sa légitime défense en cas d'agression, pour porter assistance à un autre État de l'Union européenne en application de l'article 42-7 du Traité UE, pour aider un de ses alliés en application de l'article 5 du Traité de l'Atlantique Nord, dans le cadre de la mise en œuvre d'une résolution du Conseil de sécurité de l'Organisation des Nations Unies (ONU) ou encore avec le consentement de l'État hôte. Elle doit pour ce faire avoir les moyens d'assurer la défense de sa population, de son territoire et de ses intérêts, de répondre à ses engagements conventionnels d'assistance et d'agir contre des forces hostiles, étatiques ou non étatiques, dans tous les champs et dans tous les milieux.

Principe n°2 : La défense est le premier devoir de l'État, lequel dispose du monopole de la force légitime, mais toute la Nation se doit d'y contribuer. Si l'armée de la République est au service de la Nation et si sa mission est d'assurer la défense de la Patrie, les citoyens, les entreprises et les organisations de la société civile ne sont pas des « consommateurs de sécurité » mais doivent être des acteurs de la défense et de la sécurité nationale.

Principe n°3 : Il n'y a pas de « guerre juste » sans une juste cause et de justes moyens. Ni la légitime défense, ni une résolution du Conseil de Sécurité de l'organisation des Nations Unies (ONU) ne sont susceptibles de justifier des infractions aux règles du droit des conflits armés, dont le respect constitue une des valeurs fondamentales de la République.

Principe n°4 : Les opérations conduites par les forces armées, l'emploi de la force des armes par celles-ci et les armes utilisées sont exclusivement régis, d'une part, par les règles du droit international humanitaire (DIH) fixées par les conventions internationales auxquelles la France a consenti dès lors qu'elles s'inscrivent dans une situation de conflit armé, d'autre part, par la Constitution de la République, les lois et décrets édictés par le Parlement et le gouvernement français. Les technologies d'intelligence artificielle utilisées dans ou pour les opérations militaires sont soumises au même régime juridique.

Principe n°5 : Les recherches relatives aux systèmes d'intelligence artificielle destinés à des usages offensifs comme défensifs, doivent pouvoir être conduites en toute responsabilité. Ces recherches doivent s'accompagner d'une réflexion éthique, en particulier sur la portée et les développements possibles de leurs résultats.

Principe n°6 : Le développement et le déploiement de technologies d'intelligence artificielle appliquées à la médecine militaire doivent suivre les règles éthiques et déontologiques propres au domaine médical

et à la recherche en santé. Ces technologies devront préserver l'autonomie de décision du personnel de santé afin de garantir la meilleure qualité et la sécurité des soins.

Principe n°7 : Les systèmes intégrant des technologies d'intelligence artificielle doivent être associés à des cas d'utilisation définis, pour lesquels ils ont été testés, vérifiés et validés, voire certifiés. La révision de ces vérifications avec les évolutions des systèmes et de leurs usages doit être envisagée avec une fréquence adaptée aux enjeux.

Principe n°8 : Si les apports des technologies d'intelligence artificielle peuvent être utiles voire nécessaires, la décision humaine dans l'utilisation de systèmes intégrant de telles technologies doit être liée au contexte, selon que l'environnement est hostile ou non, permissif ou non, et doit rester subordonnée à l'appréciation de situation qui est de la responsabilité du commandement, au niveau stratégique, opératif ou tactique.

Principe n°9 : Si la subsidiarité doit prévaloir pour que la décision humaine soit prise au bon niveau d'appréciation de la situation et au bon moment, cette décision doit être accompagnée d'un compte rendu à l'autorité supérieure.

Les recommandations du Comité

Recommandation n°1 : Des modalités adaptées de contrôle de licéité doivent être appliquées tenant compte des enjeux nouveaux que peut induire l'utilisation de certaines technologies d'intelligence artificielle dans les armes, les systèmes d'armes et les opérations.

Recommandation n°2 : Les systèmes intégrant des technologies d'intelligence artificielle doivent être évalués et qualifiés, au juste niveau, c'est-à-dire selon des exigences proportionnées aux bénéfices que l'on veut tirer et aux risques que l'on veut éviter.

Recommandation n°3 : Il importe que l'entraînement et le test des modèles d'intelligence artificielle destinés aux armées s'appuient sur des données maîtrisées et, autant que possible, appliquées à leur usage militaire et au niveau de souveraineté souhaité. Pour autant l'interopérabilité avec nos alliés doit être dans toute la mesure du possible préservée. Cette maîtrise et cette souveraineté des données constituent un investissement dont il faut accepter le prix.

Recommandation n°4 : De façon générale, les formations accompagnant la mise en place de systèmes intégrant des technologies d'intelligence artificielle doivent permettre la sensibilisation aux risques de sécurité des systèmes d'information.

Recommandation n°5 : Il importe de mener des études d'ergonomie prenant en compte les conditions réelles d'utilisation de systèmes intégrant des technologies d'intelligence artificielle dans le cadre des opérations, y compris en conditions dégradées.

Recommandation n°6 : Les critères d'acceptation de l'automaticité variant selon les circonstances, les technologies d'intelligence artificielle devront permettre, le cas échéant, de faire varier le niveau d'automatisation de certaines fonctions selon l'appréciation du commandement et de ses délégataires.

Recommandation n°7 : La formation des militaires doit favoriser leur compréhension des documents de transparence et surtout favoriser leur capacité à détecter que la fonction assurée par une technologie d'intelligence artificielle est dégradée, polluée ou insuffisante et qu'il est nécessaire de reprendre la main.

Recommandation n°8 : Les militaires doivent continuer d'être formés aux fondamentaux et aux savoir-faire de leurs métiers afin de leur permettre d'agir ou de combattre en mode dégradé ou en l'absence des technologies d'intelligence artificielle.

Recommandation n°9 : Il importe de formaliser les chaînes de responsabilité du commandement, du contrôle et de l'exécution quelles que soient les fonctions réalisées par le système intégrant des technologies d'intelligence artificielle.

Recommandation n°10 : Les responsabilités humaines (des industriels, annotateurs, programmeurs, utilisateurs, superviseurs, décideurs…) doivent être clairement définies afin qu'elles puissent être assumées dans l'emploi de la force.

Recommandation n°11 : Il importe de sensibiliser les opérateurs à la nécessité du retour d'expérience sur l'utilisation des systèmes d'intelligence artificielle.

Recommandation n°12 : Des études doivent être menées concernant l'impact dans la durée des technologies d'intelligence artificielle sur les organisations et sur les relations entre humains.

TABLE DES MATIERES

Préambule

(8) Le Comité d'éthique de la défense a été saisi, par le ministre des Armées, d'une demande d'avis sur « l'intelligence artificielle de défense ».

(9) Pour conduire ses travaux, le Comité a procédé à l'audition de personnalités civiles et militaires et à des visites d'unités et d'organismes en lien avec le développement et l'usage de technologies d'intelligence artificielle.

(10) **L'intelligence artificielle (IA) est une discipline fondée notamment sur les mathématiques** en vue de simuler des facultés mentales humaines avec des machines. Elle regroupe un ensemble de techniques fondées sur la modélisation de connaissances et sur l'exploitation de données.

a. Tel est le sens de la définition du JORF du 9 décembre 2018 (texte n°58) : « ***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 et logiciel, à des fins d'assistance ou de substitution à des activités humaines*** ».

b. Tel est également le sens de la définition retenue, six ans plus tard, par le Règlement (UE) 2024/1689, dit « *AI Act* », du 13 juin 2024 en son article 3 §1 [3]

(11) Les **progrès spectaculaires réalisés dans la dernière décennie notamment avec l'apprentissage profond, l'explosion du volume des données, le développement de grands modèles de langue et l'essor de l'intelligence artificielle générative, ont permis de multiplier les usages de l'intelligence artificielle** dans l'industrie, la banque, les transports, l'énergie, le commerce, la recherche, la santé et plus généralement dans la société et notre vie quotidienne. Des technologies d'intelligence artificielle ont parallèlement été développées pour accroître les moyens de surveillance et de sécurité mais aussi, dans les régimes politiques autoritaires, les instruments de contrôle et de répression des populations.

On mesure bien là **l'ambivalence de l'intelligence artificielle et de ses usages, innovation** qui, comme d'autres innovations dans le passé, est porteuse d'espoirs pour l'humanité mais suscite aussi des craintes pour le travail, les rapports sociaux, les droits et libertés, la paix et la stabilité dans le monde.

Du fait des enjeux et des intérêts en cause, **l'intelligence artificielle est devenue le champ d'une compétition scientifique et économique mondiale mettant aux prises les États comme les entreprises.**

(12) **La France, puissance de premier rang**, qui peut s'appuyer sur un écosystème d'ingénieurs de talent, d'entreprises performantes et qui bénéficie d'une énergie électrique nationale, largement décarbonée et compétitive, **s'est dotée d'une *« Stratégie nationale en intelligence artificielle »* pour éviter tout décrochage et devenir un pays pionnier en matière d'intelligence artificielle.**

(13) Cette stratégie nationale s'est déployée en trois phases en vue de mobiliser les moyens financiers, de faire émerger les talents et de doter notre pays des infrastructures essentielles [4]:

- 2018 : la première phase, « *AI for humanity* », a été lancée par le président de la République.
- 2022 : la stratégie a été renforcée, dans le cadre de France 2030, pour diffuser plus largement les usages de l'IA et former davantage de talents.

[3] Site de l'Union européenne, Règlement (UE) 2024/1689. https://eur-lex.europa.eu/legal-content/FR
[4] Site du ministère de l'enseignement supérieur et de la recherche, La stratégie française en intelligence artificielle, https://www.enseignementsup-recherche.gouv.fr/fr/la-strategie-francaise-en-intelligence-artificielle-49166

- 2023 : un volet complémentaire, consacré à l'intelligence artificielle générative, a été défini afin d'accompagner et d'accélérer le développement de nos champions nationaux.

(14) Parallèlement**,** et **alors que dans le monde des puissances militaires, parmi nos alliés comme parmi des acteurs étatiques et non étatiques qui nous sont hostiles, ont engagé des programmes visant à leur conférer, grâce aux technologies de l'intelligence artificielle, l'ascendant opérationnel, la République ne pouvait, en aucun cas et à aucun prix, tenir les armées françaises à l'écart de recherches et de développements permettant de garantir notre souveraineté, notre indépendance et le respect de nos engagements internationaux.**

(15) À cet effet, la **stratégie française pour l'intelligence artificielle de défense a été engagée en 2019** [5] **puis amplifiée et développée dans une instruction du ministre des Armées, en date du 18 janvier 2024, définissant la « S*tratégie ministérielle pour l'intelligence artificielle* » à mettre en œuvre dans l'ensemble des armées, directions et services du ministère des Armées.** Cette stratégie, dont l'objectif est d'accélérer l'utilisation d'une intelligence artificielle de défense, a été dévoilée, le 8 mars 2024, par le ministre des Armées, Sébastien Lecornu[6]. Le 1er mai 2024, **l'agence ministérielle pour l'intelligence artificielle de défense (AMIAD) a été créée afin d'assurer une maîtrise souveraine des technologies de l'intelligence artificielle par le ministère des Armées.**

******

C'est dans ce contexte que le Comité d'éthique de la défense a été saisi par le ministre des Armées d'une demande d'avis sur l'intelligence artificielle et la défense.

Le présent avis fait suite aux avis du Comité sur l'intégration de l'autonomie dans les systèmes d'armes létaux du 29 avril 2021 et sur l'environnement numérique des combattants du 13 avril 2022.

Cet avis est rendu en l'état des connaissances des technologies d'intelligence artificielle.

******

[5] Discours de la Ministre à Saclay, le 5 avril 2019 (https://www.vie-publique.fr/discours/271295-florence-parly-5042019-intelligence-artificielle-et-defense) et rapport de la *Task force IA* de septembre 2019 « *l'intelligence artificielle au service de la défense* ».

[6] Discours du Ministre à Palaiseau, le 8 mars 2024 (https://www.vie-publique.fr/discours/293389-sebastien-lecornu-08032024-intelligence-artificielle)

I. La défense est au service de la République et de ses valeurs

(16) La France **aspire à la paix et ne menace personne.** Sa Constitution dispose d'ailleurs : *« La République française, fidèle à ses traditions, se conforme aux normes du droit public international. Elle n'entreprendra aucune guerre dans des vues de conquête et n'emploiera jamais ses forces contre la liberté d'aucun peuple* [7]*»*.

(17) **Attachée au multilatéralisme et à un ordre international fondé sur le droit**, **membre fondateur de l'Organisation des Nations Unies et membre permanent de son Conseil de Sécurité, la France n'entend recourir à la force sur le territoire d'un autre État que dans le strict respect de la légalité internationale** :

- avec le consentement de l'État sur lequel l'intervention a lieu ;
- sur la base d'une résolution du Conseil de sécurité, sous chapitre VII de la charte des Nations Unies : action en cas de menace contre la paix, la rupture de la paix et d'acte d'agression [8] ;
- dans le cadre de la légitime défense individuelle ou collective en cas d'agression armée au sens de l'article 51 de la charte des Nations Unies.

(18) **Cependant, il ne suffit pas de vouloir la paix pour être en paix**. Le terrorisme demeure un grave danger. Les États proliférants continuent à défier l'ordre international garanti par des traités fragilisés. Enfin, la paix du monde, notre indépendance et notre sécurité sont menacées par les actions, ouvertes ou souterraines, y compris sur notre continent, de puissances militaires ou de groupes non-étatiques hostiles, voire désinhibés, auxquelles les technologies d'intelligence artificielle peuvent donner une nouvelle ampleur.

(19) **Assurer notre défense et, par là-même, participer à la stabilité du monde sont des impératifs absolus**.

> ***Principe n°1*** **: La France n'entend recourir à la force des armes que dans le respect de la légalité internationale pour assurer sa légitime défense en cas d'agression, pour porter assistance à un autre État de l'Union européenne en application de l'article 42-7 du Traité UE, pour aider un de ses alliés en application de l'article 5 du Traité de l'Atlantique Nord, dans le cadre de la mise en œuvre d'une résolution du Conseil de sécurité de l'Organisation des Nations Unies (ONU) ou encore avec le consentement de l'État hôte. Elle doit pour ce faire avoir les moyens d'assurer la défense de sa population, de son territoire et de ses intérêts, de répondre à ses engagements conventionnels d'assistance et d'agir contre des forces hostiles, étatiques ou non étatiques, dans tous les champs et dans tous les milieux.**

(20) La **défense participe étroitement de la sauvegarde des intérêts fondamentaux de la Nation** au nombre desquels figurent l'indépendance nationale, l'intégrité du territoire, la protection de la population. Ce sont là des **obligations constitutionnelles qui s'imposent à toutes les autorités publiques et d'abord à l'État dont c'est le premier devoir, en même temps qu'à tous les citoyens, de même qu'à tous les acteurs publics et privés.**

> ***Principe n°2*** **: La défense est le premier devoir de l'État, lequel dispose du monopole de la force légitime, mais toute la Nation se doit d'y contribuer. Si l'armée de la République est au service**

[7] Préambule de la Constitution du 27 octobre 1946 maintenu en vigueur par la Constitution du 4 octobre 1958.
[8] Par exemple, intervention aux cas de génocide, de crime de guerre, de nettoyage ethnique et de crimes contre l'humanité.

de la Nation et si sa mission est d'assurer la défense de la Patrie, les citoyens, les entreprises et les organisations de la société civile ne sont pas des « consommateurs de sécurité » mais doivent être des acteurs de la défense et de la sécurité nationale.

(21) **La défense est une impérieuse obligation mais, au service de cette défense, tous les moyens ne sont pas admissibles tant au regard des lois de la République que du droit international.**

(22) **D'une part, la France a ratifié la plupart des conventions internationales applicables en situation de conflit armé ainsi que celles prohibant ou restreignant la fabrication, la détention et l'utilisation de certaines armes,** c'est-à-dire les règles de droit international qui, pour des raisons humanitaires, visent à limiter les effets des hostilités ou qui ont pour finalité d'assurer la protection des victimes de ces conflits armés. Ces conventions engagent pleinement l'État, les autorités publiques et les forces armées françaises. **Certaines des normes ou interdictions qu'elles comportent correspondent, au demeurant, à des principes ou des valeurs inhérentes au corpus éthique de l'armée française.** (*cf.* l'avis du comité d'éthique de la défense relatif à « l'éthique dans la formation des militaires »).

(23) **D'autre part le droit pénal français a transposé dans notre ordre interne certaines obligations conventionnelles, en réprimant spécialement les crimes contre l'humanité [9]ainsi que les crimes et délits de guerre commis lors des conflits armés internationaux et non-internationaux,** notamment à l'encontre des personnes protégées par le droit international, les crimes et délits de guerre liés à la conduite des hostilités, l'utilisation de moyens ou méthodes de combat prohibés [10].

(24) **Enfin le législateur a édicté le statut général des militaires, lequel impose à ceux-ci des sujétions exceptionnelles allant jusqu'au sacrifice suprême au nom de la défense de la Patrie tout en soumettant leur action au combat à des impératifs éthiques rigoureux et au respect du droit des conflits armés.** Le ministère des armées a notamment publié le **« Manuel de droit des opérations miliaires »** qui recense les principales règles régissant l'emploi de la force par les forces armées françaises sur le territoire national et à l'étranger, en temps de paix comme en situation de conflit.

***Principe n°3* : Il n'y a pas de « guerre juste » sans une juste cause et de justes moyens. Ni la légitime défense, ni une résolution du Conseil de Sécurité de l'organisation des Nations Unies (ONU) ne sont susceptibles de justifier des infractions aux règles du droit des conflits armés, dont le respect constitue une des valeurs fondamentales de la République.**

II. Les technologies d'intelligence artificielle jouent déjà un rôle et sont appelées à l'avenir à jouer un rôle croissant dans notre défense

(25) **Par l'effet de notre Constitution et des principes qui en sont issus, nos opérations militaires, les armes utilisées par nos armées et l'emploi de la force des armes par celles-ci en situation de conflit armé (international ou non-international) sont exclusivement régis, d'une part, par les règles du droit international humanitaire (DIH), d'autre part, par les lois et décrets édictés par le Parlement et le gouvernement français.**

[9] Articles 211-1 à 213-4-1 du code pénal.
[10] Articles 461-1 à 461-31 et 462-1 à 462-11 du code pénal.

(26) **Ce régime est celui qui est applicable à tous les engagements militaires des forces armées de la République, c'est-à-dire l'armée de Terre, la Marine nationale, l'armée de l'Air et de l'Espace, la Gendarmerie nationale ainsi que les formations rattachées**.

(27) **Les technologies d'intelligence artificielle utilisées dans ou pour les opérations militaires sont soumises au même régime juridique**.

(28) Il est à noter, d'ailleurs, que **le Règlement (UE) du 13 juin 2024 dit « *AI Act* » prend soin, comme il le devait, de placer les systèmes d'IA militaires hors de son champ d'application** (ce qui couvre, au sens de ce règlement, les *« systèmes d'IA mis sur le marché, mis en service ou utilisés avec ou sans modification de ces systèmes à des fins militaires, de défense ou de sécurité nationale »* (cf. §24 et article 2), **cette exclusion étant expressément motivée par la compétence exclusive des États membres dans ces deux domaines, en vertu de l'article 4 §2 du Traité sur l'Union européenne et par la prévalence du Droit international public.**

> ***Principe n°4*** **: Les opérations conduites par les forces armées, l'emploi de la force des armes par celles-ci et les armes utilisées sont exclusivement régis, d'une part, par les règles du droit international humanitaire fixées par les conventions internationales auxquelles la France a consenti dès lors qu'elles s'inscrivent dans une situation de conflit armé, d'autre part, par la Constitution de la République, les lois et décrets édictés par le Parlement et le gouvernement français. Les technologies d'intelligence artificielle utilisées dans ou pour les opérations militaires sont soumises au même régime juridique.**

(29) Les applications militaires des technologies de l'intelligence artificielle peuvent être des facteurs de rupture **dans les différents domaines et milieux de conflictualité et constituer, pour ceux qui en ont la maîtrise, des atouts opérationnels.**

(30) Ainsi que le soulignait le rapport de septembre 2019 «***L'intelligence artificielle au service de la défense»*** de la Task Force IA[11], les technologies d'IA offrent des potentialités au service de la supériorité opérationnelle :

- **Mieux comprendre et élaborer la situation, anticiper et planifier, décider plus vite**. Les technologies d'IA permettent un raccourcissement de la « « boucle décisionnelle », Observation-Orientation-Décision-Action (OODA), et de la « boucle du renseignement » Orientation-Recueil-Évaluation-Diffusion (ORED), via une analyse plus complète et plus rapide des situations qu'un traitement humain, grâce à des analyses croisées de données massives ;
- **Mieux protéger nos soldats, mieux les entraîner**. Les technologies d'IA permettent d'augmenter l'efficacité des systèmes d'armes, mais aussi de favoriser la formation et le soutien du combattant ainsi que de contribuer à la préservation de la santé des soldats ;
- **Favoriser le respect du droit international humanitaire (DIH) en permettant une meilleure appréciation de l'environnement des opérations à un niveau tactique, opératif et stratégique**. Les technologies d'intelligence artificielle permettent d'améliorer la discrimination entre combattants et non-combattants, de renforcer la proportionnalité en maîtrisant les effets des armes en fonction de la menace, de garantir une action déterminée par la stricte nécessité ;
- **Libérer l'humain de tâches chronophages ou répétitives** ;

[11] Rapport de la Task Force IA, https://www.vie-publique.fr/rapport/270333-lintelligence-artificielle-au-service-de-la-defense

- **Gérer des flux d'informations plus importants et plus complexes**. Les technologies d'intelligence artificielle permettent d'apporter des solutions de calcul pour optimiser des flux et des ressources.

(31) **Les cas d'usage possibles pour les armées couvrent un large spectre d'activités à travers des systèmes d'intelligence artificielle embarqués ou non dans les plateformes et armements,** concourant notamment et de façon non exhaustive à :

a. L'aide à la préparation opérationnelle (dont formation et entraînement).

   Par exemple le système *IA FPN*, visant à maximiser les chances de succès de la formation des pilotes (présenté par l'AMIAD lors du salon EuroSatory 2024). Face à l'exigence, à la durée et au coût de la formation des personnels navigants, l'enjeu de ce système est d'alerter les instructeurs suffisamment tôt et de cibler les efforts à réaliser pour surmonter les difficultés que l'élève pilote rencontre et ainsi maximiser ses chances de succès, grâce à une analyse des données recueillies lors des formations (vol ou simulation).

b. L'aide au renseignement ;

   Par exemple, un système exploitant des images satellitaires ou de reconnaissance aérienne pour présélectionner des objets d'intérêt au profit des analystes, mais aussi fusionnant ces données images avec des données textuelles de situation opérationnelle dans l'objectif de présenter aux commandants d'entités de renseignement des synthèses de situation.

c. L'aide à la surveillance et la sûreté, voire la surveillance ;

   Par exemple le système Oreille d'or, traitant massivement des données acoustiques pour en faire le tri et orienter l'attention des opérateurs oreilles d'or sur les seuls signaux à valeur ajoutée, sur lesquels ils pourront apporter leur compétence métier (présenté par l'AMIAD lors du salon EuroSatory 2024).

d. L'aide à la décision, voire la décision pour la planification ;

   Par exemple dans une phase d'observation, des systèmes traitant une quantité importante de données captées sur une durée longue permettant de dissiper d'autant le brouillard de la guerre (activité suspecte, présence d'éléments détectés, présence de civils) et de déterminer le point clé de la manœuvre à effectuer. Dans la phase d'orientation, ces systèmes permettraient d'offrir une meilleure grille de compréhension et d'analyse d'une situation dans un environnement opérationnel évolutif et complexe, en capitalisant les données précédemment et actuellement récoltées.

   Autre exemple, un système qui aiderait au choix d'un plan d'opération en simulant un déroulement confrontant différentes options aux modes d'actions ennemis.

e. L'aide au ciblage, voire le ciblage ;

   Par exemple des capacités de traitement en temps réel de données opérationnelles pour renforcer la fiabilité de l'évaluation des dommages collatéraux et améliorer la précision et/ou le choix de l'armement envisagé pour réaliser l'intervention.

f. L'aide à la décision, voire la décision pour le combat (évaluation de situation, conseils de manœuvre ou de tir …) ;

   Par exemple, le système DeMAIA appuyant les équipages dans la veille optique des véhicules Griffon (présenté par l'AMIAD lors du salon EuroSatory 2024). Face à la difficulté pour l'équipage d'exploiter les images des six caméras retransmises dans l'habitacle, le système DeMAIA est capable de repérer des matériels ou des hommes jusqu'à trois kilomètres des capteurs y compris en lisière de forêt. Pour les opérateurs, cela se matérialise par un rectangle rouge autour des éléments détectés qu'ils peuvent suivre en temps réel.

g. L'aide à la gestion du combat collaboratif voire la gestion du combat collaboratif / la robotique dans les milieux terre/air/mer/espace (y compris les drones, les essaims) ;

   Par exemple des programmes récoltant et traitant un grand nombre de données issues des véhicules (terrestres, aériens et /ou navals) pour proposer des trajectoires en environnement hostile maximisant les chances de survie, des solutions de traitement de menaces, d'attribution des tâches, etc.

h. L'aide à la cybersécurité ;

   Par exemple, des systèmes optimisant les processus de lutte informatique défensive, de recherche de failles automatisée ou de traitement de masses de données, dans l'objectif de rendre la défense des systèmes d'information et des systèmes d'armes plus efficace et plus réactive face à un incident.

i. L'aide à la lutte informationnelle ;

   Par exemple un système de détection des *deepfakes* et des informations mensongères contre les forces armées (présenté par l'AMIAD lors du salon EuroSatory 2024). Face aux capacités de production de fausses informations par des systèmes d'intelligence artificielle et aux graves répercussions que peuvent en avoir les diffusions sur les réseaux sociaux ou Internet, un tel outil consolide le travail des opérateurs en décelant des passages falsifiés dans des supports vidéo, images ou audio, pour faciliter une exploitation opérationnelle (dénonciation par exemple).

j. Le renforcement du soutien (maintien en condition opérationnelle (MCO), soutien du combattant, …) ;

   Par exemple le système Resistance de traduction instantanée des langues étrangères sur smartphone (présenté par l'AMIAD lors du salon EuroSatory 2024) a pour objectif de permettre, en opération, hors-connexion et sans réseau, de communiquer avec les populations civiles et les autorités locales et de répondre ainsi à cette nécessité quotidienne, particulièrement lorsque la présence d'un traducteur humain n'est pas assurée.

   Autre exemple le système Rora, d'identification rapide de pièces détachées (présenté par l'AMIAD lors du salon EuroSatory 2024). Face à des pièces parfois complexes à identifier, cette application permet d'identifier une pièce avec exactitude grâce à une simple photo pour faire gagner du temps aux opérateurs de maintenance et limiter les risques de retards de maintenance et d'approvisionnement.

k. L'aide à la conception / rédaction (systèmes d'armes, fiches d'état-major, …) ;

   Par exemple des systèmes interrogeant les données disponibles au sein des états-majors pour produire des fiches de synthèse thématiques à soumettre aux traitants.

(32) **Eu égard aux enjeux stratégiques et opérationnels, les recherches relatives aux systèmes d'intelligence artificielle, destinés à des usages offensifs comme défensifs, doivent pouvoir être conduites en toute responsabilité et ce afin de préserver voire d'accroître les capacités de nos forces armées. Ces recherches doivent s'accompagner d'une réflexion éthique, en particulier sur la portée et les développements possibles de leurs résultats.**

(33) L'objet et l'horizon des programmes de recherche doivent être ouverts sans que soient édictés a priori des interdits. Nous avons besoin pour protéger nos forces de connaître les dispositifs que l'ennemi pourrait utiliser même si, pour des raisons éthiques, nos forces, elles, ne le pourraient pas.

Principe n°5 **: Les recherches relatives aux systèmes d'intelligence artificielle destinés à des usages offensifs comme défensifs, doivent pouvoir être conduites en toute responsabilité. Ces recherches doivent s'accompagner d'une réflexion éthique, en particulier sur la portée et les développements possibles de leurs résultats.**

Principe n°6 **: Le développement et le déploiement de technologies d'intelligence artificielle appliquées à la médecine militaire doivent suivre les règles éthiques et déontologiques propres au domaine médical et à la recherche en santé. Ces technologies devront préserver l'autonomie de décision du personnel de santé afin de garantir la meilleure qualité et la sécurité des soins.**

(34) Si des technologies d'intelligence artificielle devaient être employées dans le domaine de l'augmentation du combattant, il conviendra, conformément à la doctrine du ministère en la matière, de respecter le principe de dignité de la personne humaine, de s'assurer de l'innocuité des interventions envisagées et de garantir la préservation de la santé physique et psychique des militaires[12].

(35) Les cadres juridiques national et européen sont, en première analyse, favorables au développement de technologies d'intelligence artificielle à usage ou finalité militaire, y compris lorsqu'elles sont initialement conçues et développées à des fins civiles puis, dans un second temps, utilisées par les armées. Il y aurait lieu cependant de bien mesurer **l'impact à terme sur l'industrie et la recherche européenne que peut avoir** un règlement qui, comme le Règlement (UE) du 13 juin 2024 comporte 257 pages, dont 89 pages de considérations générales et de définitions, 113 articles et 13 annexes normatives, **le risque étant « *in fine* » un décrochage de la recherche et de l'industrie européenne avec comme conséquence, pour les armées françaises et la défense européenne, de n'avoir qu'une seule option : *« l'IA des autres »***.

(36) Il y aurait lieu de même d'évaluer les impacts éventuels des usages de technologies d'intelligence artificielle dits « organiques » (ressources humaines, finances, logistique) afin de permettre la mise en commun de certaines de ces données pour des traitements au profit d'opérations.

(37) Il conviendrait ainsi de prêter attention aux risques d'introduction de normes ou de règles civiles dans les programmes d'intelligence artificielle organiques et qui constitueraient un frein aux opérations.

(38) L'examen des cas d'usage possibles fait apparaître des enjeux de licéité et de responsabilité (concepteur, commandement, opérateur) ainsi que des questions de sûreté de fonctionnement (incertitudes, erreurs et défaillances), et de désinhibition (par la création d'une distance entre le terrain et le combattant).

III. Une bonne maîtrise des usages militaires de l'intelligence artificielle est nécessaire et possible

(39) **Il convient de rappeler que les technologies d'intelligence artificielle militaires couvrent un périmètre bien plus large que les systèmes d'armes autonomes (SAA) avec lesquels elles ne doivent pas être confondues. Par suite les usages de technologies d'intelligence artificielle militaires doivent, en tant que besoin, être entourées de garanties particulières : garanties de licéité, garanties de conception, garanties de mise en œuvre, garanties de log cours.**

[12] Cf. avis du comité d'éthique de la défense du 18 septembre 2020 portant sur « le soldat augmenté ».

A. Le contrôle de licéité

(40) **Une technologie d'intelligence artificielle ne constitue pas en soi une arme. Par voie de conséquence, elle n'est pas susceptible d'être regardée comme une arme illicite susceptible d'être prohibée par une convention internationale**.

(41) **En revanche certains usages de technologies d'intelligence artificielle à des fins militaires et les conditions d'emploi de ces technologies peuvent, dans certains cas, être regardés comme des méthodes et des moyens de combat dont les effets ne pourraient pas être limités et qui, de ce fait, sont prohibés par le droit des conflits armés (DCA).** En effet les conflits récents se déroulant sur le flanc Est de l'Europe ou au Moyen-Orient ont tous deux démontré les apports opérationnels comme les risques engendrés par l'emploi de matériels intégrant des technologies d'intelligence artificielle en situation de conflit armé.

(42) Se pose dès lors la question de la conformité au DIH de certains systèmes intégrant des technologies d'intelligence artificielle, en vertu de l'article 36 du Protocole additionnel I aux Conventions de Genève du 12 août 1949 relatif à la protection des victimes des conflits armés internationaux du 8 juin 1977 (PA I). Celui-ci dispose en effet que « *dans l'étude, la mise au point, l'acquisition ou l'adoption d'une nouvelle arme, de nouveaux moyens ou d'une nouvelle méthode de guerre, une Haute Partie contractante a l'obligation de déterminer si l'emploi en serait interdit, dans certaines circonstances ou en toutes circonstances, par les dispositions du présent Protocole ou par toute autre règle du droit international applicable à cette Haute Partie contractante* ».[13]

(43) Respectueuse de ses engagements, la France a précisé les modalités de cet examen de licéité et la façon dont cette démarche d'analyse de conformité au droit international accompagne toutes les phases de déroulement d'une opération d'armement. Le Comité souligne en particulier que cet examen est conduit, en tant que de besoin, lors des différentes phases du cycle de vie d'un système d'armes : en phase de préparation, de réalisation mais aussi d'utilisation opérationnelle. Au cours de cette dernière phase qui est souvent la plus longue, l'examen est prévu dès lors que « le traitement d'obsolescences, l'intégration d'innovations de l'arme, du moyen, ou de la doctrine contribuent à une évolution des fonctions pouvant remettre en cause l'avis de licéité précédent ».[14]

(44) Compte tenu des risques évoqués précédemment, le Comité souligne l'importance et la pertinence d'un examen de licéité de bout en bout lorsqu'une technologie d'intelligence artificielle est développée ou intégrée dans un système utilisé par les forces armées, en particulier dans des fonctions comme l'identification, la classification ou l'ouverture du feu.

(45) Il est donc indispensable conformément aux procédures ministérielles d'appliquer des modalités adaptées aux enjeux nouveaux que peut induire l'utilisation de certaines technologies d'intelligence artificielle dans les armes, les systèmes d'armes et les opérations.

(46) Il appartient ensuite aux responsables de décider de leur déploiement et de leur usage dans le respect de l'approche éthique ici proposée.

Recommandation n°1 **: Des modalités adaptées de contrôle de licéité doivent être appliquées tenant compte des enjeux nouveaux que peut induire l'utilisation de certaines technologies d'intelligence artificielle dans les armes, les systèmes d'armes et les opérations.**

[13] Avis du Comité du 6 janvier 2021 sur l'intégration de l'autonomie dans les systèmes d'armes létaux §126
[14] Avis du Comité du 6 janvier 2021 sur l'intégration de l'autonomie dans les systèmes d'armes létaux §128

B. Les garanties au stade de la conception

a. Sûreté de fonctionnement des technologies d'intelligence artificielle et qualification adaptée aux risques liés à l'utilisation de ces technologies.

(47) La sûreté de fonctionnement implique que les applications des technologies d'intelligence artificielle soient associées à des cas d'utilisation définis, pour lesquels elles ont été testées et vérifiées. L'examen de la sûreté de fonctionnement fait également appel aux critères qui suivent :

- **Conformité :** la conformité d'une technologie d'intelligence artificielle signifie que les résultats du système intégrant cette technologie d'intelligence artificielle coïncident avec l'objectif pour lequel elle a été conçue, résultats eux-mêmes correspondant aux spécifications du système, qui doivent répondre aux besoins des utilisateurs.

- **Transparence** : un système intégrant des technologies d'intelligence artificielle doit être transparent aux niveaux nécessaires, c'est-à-dire présenter des éléments factuels permettant aux différents acteurs concernés (concepteur, autorité d'emploi, utilisateur…) de comprendre comment et pourquoi un résultat a été obtenu. Il est dans ce cadre important de mettre à disposition de ces acteurs de la documentation portant sur la finalité des technologies d'intelligence artificielle utilisées, sur les méthodes et raisonnements conduisant à un résultat, sur les données qui ont été utilisées pour l'entraînement et le test, sur les responsabilités dans la conception et dans la mise en œuvre ainsi que sur l'évaluation des conséquences de la mise en œuvre.

  L'intérêt pour les forces armées de disposer de critères de transparence ne se limite pas au seul fait de disposer d'éléments créditant la qualification ou non d'un système d'armes. Ces critères permettraient également de faciliter la formation des militaires, d'accompagner les réponses aux questions de chefs ou d'opérateurs au sujet des technologies d'intelligence artificielle utilisées, de mettre les armées en mesure de pouvoir justifier devant les autorités politiques du recours à telle ou telle technologie d'intelligence artificielle.

- **Robustesse** : cette exigence traduit dans quelle mesure le système d'intelligence artificielle fait, de manière fiable et précise, ce qu'il est censé faire, notamment face à des sollicitations imprévues (attaque adverse, mise en œuvre erronée), face à l'introduction de données différant de celles utilisées lors de l'entraînement du système ou en cas de défaillance (le système bascule-t-il vers des modes dégradés ? récupère-t-il ses capacités ?)

***Principe n°7* : Les systèmes intégrant des technologies d'intelligence artificielle doivent être associés à des cas d'utilisation définis, pour lesquels ils ont été testés, vérifiés et validés, voire certifiés. La révision de ces vérifications avec les évolutions des systèmes et de leurs usages doit être envisagée avec une fréquence adaptée aux enjeux.**

***Recommandation n°2* : Les systèmes intégrant des technologies d'intelligence artificielle doivent être évalués et qualifiés, au juste niveau, c'est-à-dire selon des exigences proportionnées aux bénéfices que l'on veut tirer et aux risques que l'on veut éviter.**

b. Souveraineté des données pour les technologies à base d'apprentissage machine

(48) Certains outils, au-delà des conditions d'usage, doivent apporter au chef ou au combattant des résultats d'une fiabilité élevée. Il importe ainsi, dans ces cas particuliers, que l'entraînement et le test des modèles d'intelligence artificielle destinés aux armées s'appuient sur des données maîtrisées et, autant que possible, appliquées à leur usage militaire et au niveau de souveraineté souhaité. Pour autant l'interopérabilité avec nos alliés doit être dans toute la mesure du possible préservée. Cette maîtrise et cette souveraineté des données constituent un investissement dont il faut accepter le prix.

Recommandation n°3 **: Il importe que l'entraînement et le test des modèles d'intelligence artificielle destinés aux armées s'appuient sur des données maîtrisées et, autant que possible, appliquées à leur usage militaire et au niveau de souveraineté souhaité. Pour autant l'interopérabilité avec nos alliés doit être dans toute la mesure du possible préservée. Cette maîtrise et cette souveraineté des données constituent un investissement dont il faut accepter le prix.**

c. Maîtrise des risques de cybersécurité des systèmes intégrant des technologies d'intelligence artificielle

(49) Les risques de non-conformité ou liés aux performances des systèmes intégrant des technologies d'intelligence artificielle ne sont pas les seuls qui pèsent sur leur exploitation. En effet, s'ajoutent en amont ou en cours d'utilisation de ces systèmes les risques d'atteinte :

- à l'intégrité des données, par une pollution intentionnelle ou non, qui fausserait les résultats issus de l'apprentissage ;
- à la disponibilité des données qui obérerait le fonctionnement d'une technologie d'intelligence artificielle nécessitant la comparaison avec des données de référence ;
- à la confidentialité des données et/ou des résultats par le vol d'informations sensibles.

(50) Des recommandations techniques existent telles que de :

- choisir des technologies adaptées à chaque cas d'usage;
- mettre en place des parades (tatouages, cryptographie, entraînement spécifique des modèles ...) et des défenses adaptées.

Recommandation n°4 **: De façon générale, les formations accompagnant la mise en place de systèmes intégrant des technologies d'intelligence artificielle doivent permettre la sensibilisation aux risques de sécurité des systèmes d'information.**

d. Études d'ergonomie et contrôle humain

(51) La question des interfaces humain-machine revêt une très grande importance. Par suite le Comité réitère la recommandation formulée dans son avis sur l'environnement numérique du combattant, aux termes de laquelle les facteurs humains doivent faire l'objet d'une attention toute particulière. Cette recommandation vaut pour de nombreux usages et implique des études d'ergonomie prenant en compte les conditions réelles rencontrées par le combattant dans le cadre des opérations.

(52) Analyser et caractériser le contrôle humain nécessaire et suffisant, sans pour autant brider les capacités du système intégrant des technologies d'intelligence artificielle (au risque d'en perdre le bénéfice), est une problématique complexe qui doit prendre en compte différents facteurs, humains (tels que la fatigue, le stress, la compétence, etc.), techniques (transparence, aide à la validation, etc.) et contextuels (dynamique et complexité de l'environnement).

(53) Cette analyse doit reposer sur un contexte et une doctrine d'emploi adaptés et sur des expérimentations et évaluations pointues devant permettre de garantir une place pertinente des systèmes intégrant des technologies d'intelligence artificielle et une attention suffisante et adéquate de l'humain.

Recommandation n°5 **: Il importe de mener des études d'ergonomie prenant en compte les conditions réelles d'utilisation de systèmes intégrant des technologies d'intelligence artificielle dans le cadre des opérations, y compris en conditions dégradées.**

C. La maîtrise dans la mise en œuvre

e. La place de l'humain doit être maintenue dans les processus de décision

(54) Le Comité observe que les conflits actuels en Ukraine et au Proche-Orient sont des théâtres d'emploi de systèmes d'intelligence artificielle dans des combats le plus souvent à très large échelle et de façon désinhibée. Ces conflits traduisent une évolution rapide de la manière dont les opérations sont conduites.

(55) Si un système d'intelligence artificielle a pour objet de fournir des éléments de prise de décision, l'évaluation et l'acceptation ou le refus du risque encouru doivent demeurer des prérogatives humaines.

(56) Dans un contexte de conflit armé, l'environnement opérationnel ainsi que l'intensité du conflit influent, de manière évolutive, sur le niveau d'automaticité et de délégation décidé par le commandement. Les questions de l'utilisation, de la prise de décision et de l'attribution de tâches à un système d'intelligence artificielle, et selon quel degré, sont ainsi liées à l'appréciation globale de l'environnement du système d'armes et au contexte opérationnel.

Principe n°8 **: Si les apports des technologies d'intelligence artificielle peuvent être utiles voire nécessaires, la décision humaine dans l'utilisation de systèmes intégrant de telles technologies doit être liée au contexte, selon que l'environnement est hostile ou non, permissif ou non, et doit rester subordonnée à l'appréciation de situation qui est de la responsabilité du commandement, au niveau stratégique, opératif ou tactique.**

Principe n°9 **: Si la subsidiarité doit prévaloir pour que la décision humaine soit prise au bon niveau d'appréciation de la situation et au bon moment, cette décision doit être accompagnée d'un compte rendu à l'autorité supérieure.**

(57) Dans le cadre des déploiements de technologies d'intelligence artificielle pour l'aide à la décision, au niveau tactique, opératif comme stratégique, une attention particulière doit être portée quant à l'interaction entre l'outil d'aide à la décision et le chef militaire. En effet, dans des situations de forte tension où des décisions rapides doivent être prises, l'outil doit être assez robuste pour proposer des « solutions réflexes » fiables dans le cas où le décideur serait cognitivement surchargé.

(58) Ainsi, notamment lors de situations complexes et/ou temporellement contraintes, telles que des attaques saturantes, des usages (adverses) de systèmes automatisés ou plus largement dans le cadre de combats de haute intensité, des tâches devront pouvoir être automatisées grâce à des technologies d'intelligence artificielle afin de conserver la capacité à opérer avec la réactivité et la masse nécessaires.

Recommandation n°6 **: Les critères d'acceptation de l'automaticité variant selon les circonstances, les technologies d'intelligence artificielle devront permettre, le cas échéant, de faire varier le niveau d'automatisation de certaines fonctions selon l'appréciation du commandement et de ses délégataires.**

f. La formation des chefs et des combattants

(59) Le soldat doit être entraîné pour un type de combat conforme à nos valeurs.

(60) L'emploi de technologies d'intelligence artificielle et la formation des militaires à ces emplois ne doivent en rien altérer leurs aptitudes à exercer les fondamentaux de leurs métiers qui fondent la plus-value humaine d'appréciation.

(61) Afin que ces systèmes d'intelligence artificielle s'insèrent pleinement dans une doctrine d'emploi des forces, il sera nécessaire de former les opérateurs aux limites de ces systèmes.

(62) Le chef militaire aura besoin d'un processus d'acculturation plus fort pour que les systèmes d'intelligence artificielle ne soient pas des boîtes noires pour lui, et qu'il puisse les utiliser en ayant conscience de leurs apports et de leurs limites.

(63) La formation doit avoir pour objectif de permettre le discernement et de prévenir des mésusages où l'humain se laisserait porter par les résultats proposés par les systèmes d'intelligence artificielle.

Recommandation n°7 **: La formation des militaires doit favoriser leur compréhension des documents de transparence et surtout favoriser leur capacité à détecter que la fonction assurée par une technologie d'intelligence artificielle est dégradée, polluée ou insuffisante et qu'il est nécessaire de reprendre la main.**

Recommandation n°8 **: Les militaires doivent continuer d'être formés aux fondamentaux et aux savoir-faire de leurs métiers afin de leur permettre d'agir ou de combattre en mode dégradé ou en l'absence des technologies d'intelligence artificielle.**

g. La responsabilité tout au long du cycle de vie et d'utilisation (conception, entraînement, décision, utilisation) des systèmes intégrant des technologies d'intelligence artificielle.

(64) La responsabilité ne peut pas être attribuée à un système d'intelligence artificielle.

(65) La responsabilité humaine dans la conception, le déploiement et l'emploi de technologies d'intelligence artificielle constitue un principe indérogeable. Les valeurs les plus hautes de notre civilisation comme notre ordre constitutionnel impliquent que soit engagée en toutes circonstances la responsabilité de l'humain.

Recommandation n°9 **: Il importe de formaliser les chaînes de responsabilité du commandement, du contrôle et de l'exécution quelles que soient les fonctions réalisées par le système intégrant des technologies d'intelligence artificielle.**

Recommandation n°10 **: Les responsabilités humaines (des industriels, annotateurs, programmeurs, utilisateurs, superviseurs, décideurs…) doivent être clairement définies afin qu'elles puissent être assumées dans l'emploi de la force.**

h. La dialectique du discernement

(66) Le principe du maintien de la place de l'humain dans les processus de décision implique l'acceptation d'une confrontation des résultats proposés par les systèmes intégrant des technologies d'intelligence artificielle et du raisonnement et du comportement humains.

(67) L'opérateur ou le chef militaire doit ainsi pouvoir, en toute légitimité, exercer son propre discernement, fondé sur son appréciation de situation, son expérience, son intuition, ou sur le dialogue entretenu avec son équipe ou son état-major, et doit pouvoir prendre une décision différente du résultat proposé par le système intégrant des technologies d'intelligence artificielle.

(68) Le doute quant aux résultats proposés par les systèmes intégrant des technologies d'intelligence artificielle, fruit d'une tension entre l'intuition et la déduction dans la réflexion de l'opérateur ou du chef militaire, doit être perçu comme légitime.

(69) Face au doute, il importe alors que l'éthique du chef qui n'est pas absolument sûr le conduise, lorsque cela est possible, à procéder aux vérifications qui lui sont nécessaires.

D. Les garanties nécessaires au long cours

i. Retour d'expérience

(70) Il importe de relever et de caractériser les erreurs rencontrées lors des tests ou de l'usage opérationnel d'un système intégrant des technologies d'intelligence artificielle (relever le contexte d'emploi, la nature de l'erreur, etc.).

Recommandation n°11 : Il importe de sensibiliser les opérateurs à la nécessité du retour d'expérience sur l'utilisation des systèmes d'intelligence artificielle.

j. Réentraînement des systèmes intégrant des technologies d'intelligence artificielle

(71) L'aptitude au réentraînement et à la correction du système intégrant des technologies d'intelligence artificielle avec des données réelles annotées selon leur conformité ou non à nos valeurs est cruciale. Elle le sera d'autant plus dans une dynamique où les progrès de la recherche et de la technologie permettront que la fiabilité des technologies d'intelligence artificielle aille croissant.

k. L'impact des technologies d'intelligence artificielle sur les organisations et sur les relations entre les humains

Recommandation n°12 **: Des études doivent être menées concernant l'impact dans la durée des technologies d'intelligence artificielle sur les organisations et sur les relations entre humains.**

ANNEXE

LE COMITE D'ETHIQUE DE LA DEFENSE

Le comité d'éthique de la défense a été installé le 10 janvier 2020 par la ministre des armées. Il est chargé **d'éclairer par ses avis et recommandations les autorités politiques et militaires sur les questions éthiques soulevées par les évolutions de la fonction militaire, les mutations de la conflictualité et les innovations scientifiques et technologiques dans le domaine de la défense**. Il est composé de **18 personnalités qualifiées** nommées par le ministre des armées. Leur mandat est de 3 ans, renouvelable une fois.

Composition actuelle du Comité (depuis mars 2023)

Bernard PECHEUR	Président du Comité d'éthique de la défense, président de section (h) au Conseil d'Etat.
Bernard THORETTE	Vice-président du Comité d'éthique, général d'armée (2S), ancien chef d'état-major de l'armée de terre.
Christine BALAGUÉ	Professeure à l'Institut Mines-Telecom / IMT-BS, titulaire de la Chaire Good in Tech.
Serge BARCELLINI	Président du souvenir français.
Marie-Germaine BOUSSER	Professeure émérite de neurologie, membre de l'Académie nationale de médecine.
Walter BRUYERE-OSTELLS	Professeur des universités, membre du conseil scientifique de la recherche historique de la défense.
Patrick CAREIL	Inspecteur général des finances (h).
Hervé de COURREGES	Général de corps d'armée. Directeur de l'Institut des hautes études de défense nationale (IHEDN) et de l'enseignement militaire supérieur.
Michel GOSTIAUX	Ingénieur général de l'armement.
Xavier LANDOT	Contre-amiral (2S).
Aurélie LECAM	Commissaire principale des armées.
Kévin LIMONIER	Maître de conférences, directeur-adjoint de GEODE Research center.
Ariane MICHAUD	Médecin en chef des armées.
Bruno PAUPY	Colonel de l'armée de l'Air et de l'Espace.
Guillaume SCHLUMBERGER	Administrateur général de l'État.
Catherine TESSIER	Directrice de recherche à l'ONERA, référente intégrité scientifique et éthique de la recherche de l'ONERA.
Nicolas THERY	Président des fondations du Crédit Mutuel.
Cathy THILLY-SOUSSAN	Conseillère financière, juridique et éthique de la direction générale de l'armement.

Composition antérieure (2020-2023)

Bernard PECHEUR	Président du Comité d'éthique de la défense, président de section au Conseil d'Etat (h).
Henri BENTEGEAT	Vice-président du Comité d'éthique, général d'armée (2S), ancien chef d'état-major des armées.
Christine BALAGUÉ	Professeure IMT-BS, titulaire de la chaire Good in Tech.
Rose-Marie ANTOINE	Ancienne directrice de l'Office national des anciens combattants et victimes de guerre.
Marie-Germaine BOUSSER	Professeure émérite de neurologie, membre de l'académie nationale de médecine.
Frédérick DOUZET	Professeure des Universités à l'Institut Français de Géopolitique de l'Université Paris 8 et directrice de GEODE.
Hervé DREVILLON	Directeur de recherche au sein du SHD.
Michel GOSTIAUX	Ingénieur général de l'armement.
Laurent HERMANN	Contre-amiral.
Jean-Baptiste JEANGENE-VILMER	Philosophe, juriste et politologue français.
Aurélie LECAM	Commissaire des armées, juriste.
Bruno PAUPY	Colonel de l'armée de l'Air et de l'Espace.
Philippe ROUANET DE BERCHOUX	Médecin général des armées.
Guillaume SCHLUMBERGER	Contrôleur général des armées en mission extraordinaire.
Catherine TESSIER	Directrice de recherche à l'ONERA, référente intégrité scientifique et éthique de la recherche de l'ONERA.
Nicolas THERY	Président de la Confédération Nationale du Crédit Mutuel.
Cathy THILLY-SOUSSAN	Conseillère financière, juridique et éthique de la direction général de l'armement.
Bernard THORETTE	Général d'armée (2S), ancien chef d'état-major de l'armée de terre.

Avis du Comité

Les avis du Comité d'éthique de la défense et leurs traductions sont accessibles sur le site Internet[15] :

2020 : le soldat augmenté.
2021 : l'intégration de l'autonomie dans les systèmes d'armes létaux.
2022 : l'environnement numérique des combattants
2022 : l'éthique dans la formation des militaires.
2022 : l'éthique de la défense spatiale
2024 : la place des acteurs civils dans une stratégie de défense globale

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