Consultation « Futurium » sur l'intelligence artificielle de la Commission européenne – contribution française

Les autorités françaises saluent le travail de réflexion sur l'intelligence artificielle (IA) lancé par la Commission européenne et le groupe d'experts de haut niveau qu'elle a installé. Le développement des technologies liées à l'IA, de même que les questionnements éthiques et juridiques qu'elles soulèvent, sont une priorité française. Les travaux conduits en matière d'IA aux niveaux européen et international sont ainsi suivis avec attention.

Le développement de l'IA est un objet de compétition stratégique, une course à la puissance technologique, économique mais également militaire. L'IA est en effet cruciale pour la conduite des opérations militaires de demain. Comme l'a souligné la ministre des armées dans son discours du 5 avril 2019 sur l'intelligence artificielle et la défense, « *les armées françaises investissent et investiront dans l'intelligence artificielle (…) car c'est une technologie stratégique, indispensable pour garantir notre supériorité opérationnelle. Les bénéfices potentiels de l'IA pour notre ministère sont forts et nombreux, et alors que les armées des principales puissances affûtent déjà leurs algorithmes, nous ne pouvons pas prendre le risque de manquer ce virage technologique. Tout se joue donc maintenant* ».

C'est pour satisfaire cet objectif qu'à la suite de la publication du rapport rédigé par Cédric Villani, député français, la *task force* sur l'IA du ministère des armées a publié en septembre 2019 le rapport *« l'intelligence artificielle au service de la défense »* (disponible sur www.defense.gouv.fr) détaillant la stratégie ministérielle en la matière. Une feuille de route sur l'intelligence artificielle est par ailleurs en cours d'élaboration au sein de ce même ministère et un comité ministériel sur l'éthique, présidé par un magistrat administratif membre du Conseil d'Etat français, sera mis en place avant la fin de l'année 2019, pour traiter des questions posées par les technologies émergentes et de leur emploi par l'homme dans le domaine de la défense.

Fortes de cette expérience et dans le cadre de la consultation *Futurium*, les autorités françaises souhaitent partager avec les membres du groupe d'experts de haut niveau et les institutions européennes les réflexions nationales menées dans le domaine de la défense en insistant sur quatre principaux aspects :

- le contexte et les termes de la discussion sur l'utilisation de l'IA à des fins militaires (I) ;
- la place de l'IA dans l'industrie de défense (II) ;
- l'intensification des réflexions liées à l'encadrement juridique de l'IA de défense (III) ;
- la stratégie française en la matière (IV).

* *
*

I- L'intelligence artificielle utilisée à des fins militaires : contexte et termes d'une réflexion éclairée

Le questionnaire élaboré par la Commission européenne identifie une série de technologies relevant de l'IA[1] : *1 - Supervised Machine Learning ; 2 - Unsupervised Machine Learning ; 3 - Reinforcement learning ; 4 - Robotic Process Automation ; 5 - Expert System ; 6 - Natural language processing ; 8 - Computer Vision ; 9 - Deep Learning ; 10 - Generative Adversarial Networks ; 11 - Autonomous Systems ; 12 - Distributed AI ; 13 - Ambient Computing ; 14 - Affective Computing ; 15 - Evolutionary Algorithms.*

[1] Question D6.

À ces dernières pourraient s'ajouter les technologies suivantes : - *Data Mining / Analytics ;* - *Recommender system ;* - *Anomaly Detection ;* - *Information Retrieval.*

Il ressort de la lecture de cette liste non-exhaustive que **les technologies que recouvre le concept d'intelligence artificielle soulèvent *a minima* des questions liées à la protection des libertés individuelles, en particulier la protection des données personnelles et la non-discrimination**, **aux régimes de responsabilité applicables, aux règles de concurrence, aux droits de propriété intellectuelle et industrielle ainsi qu'aux droits des consommateurs.**

Dans le domaine de la défense plus spécifiquement, les questions liées à l'usage de l'intelligence artificielle conduisent certains à examiner la problématique plus spécifique des « systèmes d'armes létaux autonomes » (SALA). Ces derniers – parfois qualifiées de « robots tueurs » par la société civile – cristallisent les opinions hostiles à l'emploi de l'IA dans le domaine de défense, au risque de la stigmatiser indument. Or, il convient de rappeler que :

- **les SALA – dont l'autonomie doit être considérée comme complète c'est-à-dire sans aucune forme de supervision humaine par opposition aux systèmes automatisés et téléopérés (tels que les drones, les torpilles ou encore les systèmes de défense automatisés) – n'existent pas**. Si de nombreuses forces armées s'appuient de longue date sur des technologies automatisées pour des séquences bien définies où les tâches n'ont pas une sensibilité nécessitant une validation humaine (tri automatique de données pour présentation à un opérateur, guidage automatique pour aller d'un point A à un point B…), le recours à des technologies autonomes n'est pas encore effectif ;

- **les applications militaires possibles de l'IA sont multiples et les innovations liées à l'IA pourraient amener des gains capacitaires significatifs dans des domaines d'application très divers**, comme l'assistance à la décision, l'amélioration des systèmes d'entraînement, l'optimisation de la maintenance ou encore la détection de cibles ou d'attaques informatiques. Il convient ici de souligner que la numérisation et la robotisation du champ de bataille n'ont pas vocation à se substituer intégralement à l'homme. Il s'agit plutôt de l'assister et d'améliorer le processus de prise de décision qui, *in fine*, doit rester centré sur le commandement humain et d'épargner à l'homme la réalisation de tâches répétitives et fastidieuses. Il s'agit également de disposer d'analyses plus rapides, plus pertinentes pour limiter au maximum les pertes civiles et militaires inutiles. Le développement de l'IA doit ainsi être perçu comme un outil d'aide à la décision pour le commandement, dans des situations opérationnelles complexes et fortement évolutives.

Dans ce contexte, il convient d'user du terme « SALA » avec précaution, d'autant plus qu'il s'agit d'un terme polysémique dont l'acception n'est pas unanimement partagée.

L'assimilation, dans les recommandations publiées par le groupe d'experts le 26 juin 2019, entre armes automatisées, dont les armées font déjà usage, et armes autonomes, qui n'existent pas, est à cet égard problématique.

Le paragraphe 28.2 des recommandations énonce en effet : « *Monitor and restrict the development of automated lethal weapons, considering not only actual weapons, but also cyber-attack tools that can have lethal consequences if deployed. With respect to offensive LAWS, advocate to the Member States to actively participate in the ongoing international debate, involve internationally recognised, non-military funded scientists and academics, experts in artificial intelligence, and propose to international partners the adoption of a moratorium on the development of offensive LAWS.* »

Plus encore, l'article 11 § 6 du règlement établissant le fonds européen de défense comporte une référence explicite aux SALA et accrédite ainsi à tort l'idée selon laquelle de tels systèmes sont utilisés

par les armées, comme le faisait la version provisoire des recommandations en matière de lignes directrices éthiques[2].

Ce manque de rigueur dans la qualification des matériels (un armement autonome ne répond pas aux caractéristiques d'un armement susceptible d'accomplir certaines missions de façon automatisée, avec un contrôle humain variable qui doit être qualifié et précisé) n'éclaire pas le débat et, de surcroît, est susceptible d'alimenter des réserves infondées à l'emploi de l'IA dans le domaine de défense, au risque notamment d'exclure du financement par des fonds européens les programmes qui y ont recours ou de décourager les investissements privés et le soutien à la recherche scientifique.

Les autorités françaises soutiennent pleinement l'ouverture de ce débat sur l'IA lancé par le groupe d'experts de haut niveau établi par la Commission européenne. Mais pour que ce débat soit éclairé il convient avant tout de s'intéresser aux systèmes qui utiliseraient ces technologies, et non pas aux technologies elles-mêmes, qui sont de nature duale et reposent sur des usages qu'il convient de circonstancier. Cette démarche exige d'envisager d'abord les usages les plus probables de l'IA dans le domaine militaire.

II- L'intelligence artificielle dans l'industrie de défense : état des lieux et perspectives

Les applications en intelligence artificielle se situent à la croisée des chemins entre les domaines applicatifs, les algorithmes et les données. Une étroite coordination entre les opérationnels, les ingénieurs, les laboratoires de recherche, les industriels spécialisés et les maîtres d'œuvres de grands systèmes est donc nécessaire pour connaitre les besoins opérationnels et les technologies disponibles, orienter les recherches spécifiques et fluidifier le transfert des laboratoires vers les acteurs spécialisés (PME, startups…) et les maîtres d'œuvres et intégrateurs du secteur de la défense.

Les grands centres de recherche sont incontournables pour détecter les pistes prometteuses, pour commencer à les faire mûrir, mais également pour valoriser des algorithmes existants sur de nouveaux cas applicatifs. En France, le Centre national de la recherche scientifique (CNRS), l'Institut national de recherche en informatique et en automatique (INRIA), le Centre d'énergie atomique (CEA), les universités et écoles d'ingénieurs, les nouveaux 3IA (instituts interdisciplinaires d'intelligence artificielle) seront des partenaires importants pour notre stratégie de développement et notre souveraineté en intelligence artificielle.

Pour les techniques de base, les sujets duaux, la défense doit s'appuyer sur des industriels spécialisés (grands groupes, établissements de taille intermédiaire, petites et moyennes entreprises et startups) qui détiennent des techniques validées sur des applications. Ces acteurs industriels peuvent valoriser leur savoir-faire et leurs algorithmes en sous-traitant des grands maîtres d'œuvres intégrateurs mais aussi réaliser des modules interfacés ou autonomes, voire fournir des solutions élémentaires dans certains cas. Ceci est particulièrement pertinent dans le cas des processus internes, où des acteurs spécialisés (entreprises du secteur numérique civil, éditeurs spécialisés) développent des offres d'analyse des données, de traitement de la voix, d'apprentissage machine pour les finances, les ressources humaines, l'assistance juridique, etc.

Les grands maîtres d'œuvres du secteur de la défense sont enfin incontournables pour la conception de modules fortement intégrés et interconnectés aux systèmes opérationnels. Il s'agit d'éviter de dupliquer inutilement des compétences rares détenues par des acteurs spécialisés qui travaillent pour le civil ou qui ont une activité duale. L'objectif est de disposer des compétences suffisantes pour leur permettre de spécifier et d'intégrer le plus rapidement possible ces technologies dans leurs systèmes. Ils devront

[2] Article 11§6 du réglement établissant un Fonds européen de defense en cours de négociation : « *Actions for the development of lethal autonomous weapons without the possibility for meaningful human control over the selection and engagement decisions when carrying out strikes against humans shall also not be eligible for financial support by the Fund, without prejudice to the possibility to provide funding for actions for the development of early warning systems and countermeasures for defensive purposes* ».

concentrer leurs efforts en capacité de développement lorsque les capteurs utilisés, les données manipulées sont spécifiquement militaires et nécessitent des développements particuliers (radars, sonars, guerre électronique, cybersécurité…).

L'ensemble des systèmes et donc des maîtres d'œuvres et fournisseurs de systèmes militaires sont concernés et seront amenés à introduire des modules d'intelligence artificielle dans leurs systèmes. Cela concerne en France autant Dassault Aviation, Naval Group, Nexter pour les systèmes de combat des avions et drones, les bâtiments de surface et sous-marins, les chars et véhicules blindés, mais également les équipementiers pour les radars, sonars, capteurs images et vidéo, missiles, systèmes de télécommunication, systèmes de guerre électronique, robots, systèmes de lutte cyber (Thales, MBDA, Airbus Defense, Safran, Eca,…). Les fournisseurs de systèmes d'information militaires dont les principaux en France sont Thales, Airbus Defense, ATOS-Bull, Sopra-Steria et Cap Gemini sont évidemment concernés au premier chef. Tous ces industriels sont conscients de l'importance du sujet et travaillent à la mise en place de feuilles de route, voire développent de manière significative leurs capacités de R&D.

De manière générale, l'industrie française de défense représente plus de 6% des emplois du secteur industriel français soit plus de 200 000 emplois, généralement de haut niveau et peu délocalisables. Le chiffre d'affaires de l'industrie de défense consolidé a été en moyenne de 20 Md€ ces dernières années, exportations incluses. La commande publique est en croissance conformément aux objectifs de la loi de programmation militaire 2019-2025. Environ 4 000 petites et moyennes entreprises, sont impliquées dans les marchés du secteur de la défense, presque toujours en sous-traitance des grands maîtres d'œuvre industriels. 500 entreprises, considérées comme stratégiques ou critiques, font l'objet d'une attention particulière du ministère des armées en raison de leur savoir-faire spécifique.

III- L'intensification des réflexions liées à l'encadrement juridique de l'IA de défense

La France soutient le développement de l'IA dans le domaine militaire. **Elle conditionne néanmoins ses usages dans ce domaine, au strict respect de trois principes** :

- le **respect du droit international en vigueur** (en particulier le droit international humanitaire – DIH) ;
- **une interaction homme-machine permettant de superviser/contrôler suffisamment le système d'arme ;**
- enfin, la **responsabilité du commandement humain**, seul responsable légitime pour définir et valider les règles de fonctionnement, d'emploi et d'engagement des systèmes d'armes.

Pour la France, il est primordial que **la prise de décision ultime sur l'emploi de la force létale reste la prérogative du commandement humain**. Cette exigence d'une décision finale reposant sur un commandement militaire organisé et subordonné aux décisions du politique est cardinale dans un Etat démocratique. Elle répond également à des exigences pénales de droit interne, ou s'agissant du respect de nos engagements internationaux (cf. le statut de Rome de la Cour pénale internationale).

La France est très engagée pour que ces principes soient reconnus et acceptés par tous. **Il est à cet égard également essentiel que ces réflexions se fondent sur les résultats des travaux menés dans le cadre de la Convention sur certaines armes classiques (CCAC), organisation internationale compétente en la matière, et en particulier son** Groupe Gouvernemental d'Experts (GGE) spécifiquement dédié à la question des SALA. Les discussions internationales démontrent d'ailleurs de manière claire la complexité du sujet et la difficulté à trouver un consensus autour de la définition des SALA, et plus généralement de la notion d'autonomie.

Dans un non-papier rédigé conjointement avec l'Allemagne et publié lors de la réunion d'août 2018 du GGE mis en place par la Conférence des États Parties à la Convention sur certaines armes classiques en 2016, la notion d'interaction homme-machine a été précisée : compréhension du système par le commandement ; subordination du système au commandement ; communication entre le système et le commandement ; contrôle du commandement sur les décisions ultimes de recours à la force létale. Plus

récemment, dans le cadre de l'Alliance pour le Multilatéralisme, la France – conjointement avec l'Allemagne – a de nouveau mis en avant le sujet des SALA.

Afin d'aboutir à une prise de position internationale sur les SALA lors de la conférence d'examen de la CCAC en 2021, la France contribue activement aux discussions en cours au sein du GGE. Les questions de la définition des SALA et de l'interaction homme - machine devraient y être centrales.

Alors que l'éventuel encadrement normatif de ces systèmes fait l'objet de plusieurs prises de position au niveau international (interdiction préventive soutenue notamment par l'Autriche et plusieurs États du mouvement des non-alignés, déclaration politique rappelant des principes généraux soutenue par la France et l'Allemagne), le GGE s'est accordé sur onze **principes directeurs** qui ont été endossés par la réunion des États Parties à la CCAC (du 13 au 15 novembre 2019), dont notamment les trois principes suivants, également identifiés par la France :

- **applicabilité du DIH aux systèmes d'armes létaux autonomes ;**
- la nécessité que les décisions d'emploi de ces systèmes relèvent toujours d'une **responsabilité humaine ;**
- le maintien d'une **interaction homme-machine qui permettra d'assurer que l'utilisation du système soit toujours conforme au DIH**, aux diverses étapes du cycle de vie de l'arme (ajout en 2019).

Des progrès substantiels ont ainsi été obtenus au sein de la CCAC, permettant de mieux délimiter les discussions à venir sur les SALA. La France considère qu'il est essentiel de les prendre pleinement en considération dans le cadres des discussions menées au niveau européen.

IV- Stratégie du ministère des armées en matière d'intelligence artificielle

L'émergence de l'intelligence artificielle et ses applications dans le domaine de la défense soulèvent légitimement des questionnements d'ordre éthique que les autorités françaises prennent très au sérieux. Consciente de ces enjeux, la France fait du développement d'une IA de défense respectueuse des droits fondamentaux une priorité absolue, défendue avec constance par la ministre des armées dans ses prises de parole, en France et à l'étranger (voir *supra*). C'est dans cet esprit que les armées abordent le développement de l'IA, technologie qui leur est indispensable dans le contexte géostratégique actuel.

Dans la course à la puissance, aux talents, à l'innovation technologique qui caractérise l'intelligence artificielle, le ministère des armées françaises a posé un diagnostic clair et ferme : l'enjeu et le rythme sont tels que tout décrochage serait irrémédiable. Il faut au contraire en tirer le bénéfice maximal pour l'Europe, les États membres et nos entreprises.

L'autonomie stratégique nationale et européenne dans le domaine numérique est l'un des objectifs incontournables pour le développement de l'IA de défense. Cela se traduit par le maintien des compétences et du savoir-faire technique permettant de réduire le risque de dépendance à des technologies non maîtrisées. Or les technologies de l'IA présentent de fortes opportunités pour accroître l'efficacité opérationnelle des forces des États membres et l'efficience de l'action de la défense en réponse aux nouvelles menaces.

La France reste toutefois parfaitement lucide : si l'IA affecte d'ores et déjà toutes les activités du ministère des Armées, que ce soit au travers d'usages spécifiquement développés pour la défense ou d'applications captées de l'innovation civile, ces technologies sont extrêmement évolutives et pour certaines peu matures. Elles ne peuvent donc en aucun cas être régulées dans la précipitation, et s'y préparer correctement est un impératif.

La stratégie du ministère des armées s'inscrit dans le cadre d'une stratégie nationale ambitieuse, pragmatique et respectueuse des valeurs de notre pays et de l'Union européenne.

Le rapport ministériel français sur l'IA *« l'intelligence artificielle au service de la défense »* a identifié quatre principes directeurs qui constituent la colonne vertébrale de la stratégie en matière d'IA de défense :

- **conserver la liberté d'action et l'interopérabilité avec nos alliés ;**
- **s'appuyer sur une IA de confiance, maîtrisée et responsable ;**
- **maintenir la résilience et l'évolutivité des systèmes ;**
- **préserver un cœur de souveraineté.**

Ces lignes directrices sont les garantes d'une IA militaire au service de la défense, capable de tirer profit des opportunités multiples offertes mais bâtie sur une attitude responsable face aux risques liés à son emploi, et notamment les risques inhérents aux spécificités du métier des armes.

a) Un développement maîtrisé et responsable

En complément du comité ministériel d'éthique précédemment cité, et afin de maîtriser les risques techniques, le ministère met en place dès à présent une « **procédure pour un développement maîtrisé de l'IA** » qui imposera des mesures de contrôle et d'audit lors de la conception, du développement et de la qualification des systèmes de défense intégrant de l'IA. Cette procédure agrègera au fil du temps les meilleures pratiques académiques et industrielles en matière d'évaluation, de métrologie et de standardisation de l'IA pour les systèmes critiques.

Les systèmes opérationnels militaires présentent en effet des caractéristiques que l'on observe seulement sur les systèmes critiques du secteur civil : nombreux systèmes embarqués ne disposant ni de liaisons haut débit entre eux ni avec des *data centers*, robotique en milieu non coopératif et non structuré, haut niveau de sécurisation des systèmes d'information et de communication, etc. De plus, la qualification[3] se pratique essentiellement sur les systèmes critiques civils (aviation, centrale nucléaire, transactions bancaires), alors qu'elle est systématique pour les systèmes opérationnels de défense, et qu'elle sera un élément clé de la maîtrise du comportement des algorithmes d'intelligence artificielle.

La robustesse des performances, les conditions à appliquer sur l'apprentissage à partir des données et les règles à suivre pour le développement devront être précisées. La transparence (au sens « boîte blanche ») est essentielle car il faut pouvoir accéder aux algorithmes et aux données d'apprentissage pour éviter les comportements cachés, vérifier les données d'apprentissage, les techniques d'IA utilisées et leur acceptabilité par rapport à la criticité de la fonction. L'absence d'apprentissage en cours de mission pour les fonctions critiques est à ce stade recommandée, avec l'enregistrement des données pour compléter l'apprentissage par incréments successifs (validés par de nouvelles qualifications). Enfin, les risques liés à l'intelligence artificielle (algorithmes et données d'apprentissage) seront pris en compte dans les études de sécurité, ce qui amènera à mettre en place une validation humaine obligatoire à certaines étapes de traitement.

Le ministère des armées conduit par ailleurs des **examens systématiques de licéité de ses nouveaux armements** afin de respecter le droit international applicable, notamment les obligations résultant du droit international humanitaire et du droit de la maîtrise des armements souscrites par la France.

b) Une gouvernance adaptée aux nouveaux enjeux

Le ministère des armées met en place une gouvernance spécifique à l'IA afin de coordonner ses actions dans le domaine. **Une cellule de coordination pour l'IA de défense a été créée au sein de l'Agence Innovation Défense du ministère durant l'été 2019.** Elle dispose à sa tête d'un coordinateur ministériel assisté d'experts pluridisciplinaires qui lui apporteront leurs compétences dans les domaines opérationnel, technologique, diplomatique, éthique ou encore juridique. Cette cellule s'appuiera par

[3] La qualification d'un système consiste à vérifier qu'un système est conforme à la règlementation applicable et aux spécifications techniques du contrat et qu'il ne présente pas de risque dans son fonctionnement avant sa mise en service.

ailleurs sur les personnels du ministère compétents en intelligence artificielle dans les armées, à la Direction Générale de l'Armement, dans les armées et dans les fonctions de soutien.

Matière première de l'IA, les données constituent le point de départ indispensable à la stratégie du ministère des armées. Ce dernier a donc rendu publique sa **politique de gouvernance de la donnée, respectant les impératifs liés aux métiers de la défense**.

c) Des axes d'effort identifiés pour soutenir les programmes structurants

La loi de programmation militaire 2019-2025, promulguée en juillet 2018, prévoit le lancement et la livraison de grands équipements structurants qui intégreront l'IA au bon niveau dans les systèmes de défense. Le ministère a déterminé des axes sur lesquels concentrer ses efforts :

- **l'aide à la décision et à la planification** car nos décideurs doivent pouvoir bénéficier des meilleures propositions dans des temps toujours plus contraints pour décider vite et juste afin d'éviter toute surprise ou méprise, et en utilisant l'ensemble des données mises à leur disposition ;
- **le renseignement,** gage majeur d'autonomie stratégique, car les moyens de recueil d'information dont nous disposons, délivrent des volumes de données conséquents. L'IA permettra de dégager l'homme des tâches non-critiques, fastidieuses et chronophages, de prendre du recul par rapport à la masse de données et de se concentrer sur des aspects critiques, opérationnels et les analyses à haute valeur ajoutée ;
- **le combat collaboratif** car la connexion déjà effective des systèmes entre eux ira croissante. Ainsi, les applications de l'IA offriront au programme SCORPION des capacités en termes de situation tactique amie et ennemie, de protection collaborative, de fusion multi-capteurs et d'optimisation des itinéraires de combat. Le programme SLAM-F bénéficiera de la détection automatique de mines dans des images sonar ou encore de la mise en œuvre des drones sous-marins et de surface avec des capacités de guidage et d'évitement d'obstacle. Enfin, la gestion assistée des capteurs et des effecteurs, la connectivité intelligente, la coopération entre aéronefs habités et drones au sein de groupes aux performances améliorées sont prévus dans la palette du SCAF[4] ;
- **la robotique** car les robots, déjà présents de manière massive dans de nombreuses entreprises, permettront de concentrer l'emploi des ressources humaines sur les tâches les plus sensibles. En matière d'armement, le domaine est particulièrement prometteur mais avancera pas à pas[5] en raison de la difficulté à automatiser le cycle complexe perception – décision – action en environnement non structuré (hors route) et non coopératif (un système de positionnement global de type Gallileo ou GPS peut être inaccessible en zone de conflit) ;
- **le cyber** car la guerre silencieuse qui se joue sur les réseaux exige toujours plus de capacité d'anticipation et de réactivité. Les attaques, à l'image des transactions boursières, se feront demain à haute fréquence, en utilisant elles-mêmes de l'IA. Pour les détecter et les contrer, les armées utiliseront l'IA pour identifier des signaux faibles et développer des stratégies défensives à grande vitesse. Dans l'espace numérique, l'IA permettra également une meilleure protection contre la propagande ou la manipulation informationnelle, deux domaines en pleine expansion, dans le sillage de la guerre hybride ;
- **la logistique, la maintenance et le soutien** constituent un domaine déjà assez mature dans le domaine civil. L'IA doit permettre de mieux prévoir l'allocation optimale des ressources et de gagner en efficacité (fonctionnement ou usure des équipements, flux logistiques, gestion des stocks, utilisation des ressources énergétiques) ;
- **dans le domaine de l'administration**, les armées bénéficieront des développements civils de l'IA pour gérer les compétences, optimiser les moyens financiers, contribuer au dépouillement de données d'essais et à la vérification de systèmes de plus en plus complexes ;

[4] SCAF : système de combat aérien futur

[5] Les experts estiment qu'il faudra probablement de l'ordre d'une dizaine d'année avant de disposer de véhicules sans conducteurs de niveau 5, c'est-à-dire tous types de routes, de conditions de circulation et de conditions atmosphériques.

- **dans le domaine de la santé** enfin, l'IA permettra de mieux diagnostiquer et prévoir l'état de santé et cognitif des militaires.

d) Un investissement de plus de 700 millions d'euros pour la recherche et l'industrie françaises

La France dispose de tous les atouts nécessaires pour une véritable stratégie concertée en matière d'IA de défense. Des partenariats stratégiques seront donc bientôt signés et plus de **700 millions d'euros d'investissements sont ainsi prévus entre 2019 et 2025**.

L'industrie et la recherche française ont des atouts considérables, en premier lieu leur capital humain. Il faut cependant noter que l'IA de défense n'est pas nécessairement celle développée par les grands groupes numériques, actuellement en pointe dans certains domaines de l'IA en raison de ses contraintes propres. En effet, l'IA pour la défense et pour les secteurs critiques (transport aérien, énergie…) doit être robuste, qualifiée, mais également comme elle est souvent embarquée, frugale en *data* et en énergie.

Par ailleurs, plus les sujets à traiter sont éloignés de cas d'usage civils (sujets et types de données) et plus la conception des chaînes algorithmiques et leur paramétrage nécessitent un effort particulier pour le secteur de la défense. La modélisation d'une situation opérationnelle est assez différente de celle du jeu de go. On manipule par ailleurs des données d'imageur thermique, de sonar de lutte sous-marine, de guerre électronique que le secteur civil ne traite pas. Ce sont ces spécificités qu'il convient dorénavant de prendre d'avantage en compte dans les travaux, déjà nombreux, qui sont conduits par la recherche et l'industrie en matière d'I.A. pour la défense.

e) Une action internationale pour donner le leadership à l'Europe

D'un point de vue stratégique, **l'Europe est l'échelle à laquelle se joue notre autonomie stratégique dans le domaine du numérique**. La stratégie ambitieuse de l'Union européenne en témoigne, en visant à lui redonner un rôle de premier plan par une coordination accrue des investissements, un soutien actif à l'innovation et une véritable politique de la donnée. Cela demeure pleinement valable pour l'utilisation de l'IA dans le domaine de la défense.

La France a déjà lancé des programmes communs intégrant de l'IA avec l'Allemagne et le Royaume-Uni. D'autres pourront suivre d'ici 2025 avec des partenaires tels que l'Espagne et l'Italie. De nombreux programmes majeurs (MGCS, SLAMF, SCAF, Space Situation Awareness) nous lient de fait, et ces partenaires resteront des piliers incontournables dans la définition d'une approche européenne incluant les sujets d'autonomie stratégique, de sécurité et de défense.

Au-delà de l'Europe, les alliés historiques de la France (États-Unis, Canada) **comme ses partenaires stratégiques** (Australie, Japon, Singapour) **sont tout autant concernés par l'introduction de l'IA** dans leurs systèmes critiques. Le programme des sous-marins australiens est un exemple de partenariat structurant et ambitieux qui incorporera des fonctionnalités d'IA. La France a également des discussions avancées avec le Japon sur la thématique des robots démineurs sous-marins. De plus, de nombreux Etats à la pointe de l'innovation et de la recherche mettent en place tout à la fois des programmes d'IA ambitieux et des mesures de contrôle destinées à s'assurer que ces développements respectent les valeurs que la France partage avec eux. Conformément à sa volonté de promouvoir une approche multilatérale des enjeux de sécurité, la France s'efforcera donc de développer un réseau de partenaires de confiance, possédant à la fois une maturité technologique et une vision du développement maîtrisé de l'IA qui soient compatibles avec la sienne, au service de la stabilité et de la sécurité internationales.

ANNEXE : Applications envisageables dans la décennie à venir (bien loin d'applications de type SALA) – source : rapport « *l'intelligence artificielle au service de la défense* » (septembre 2019)