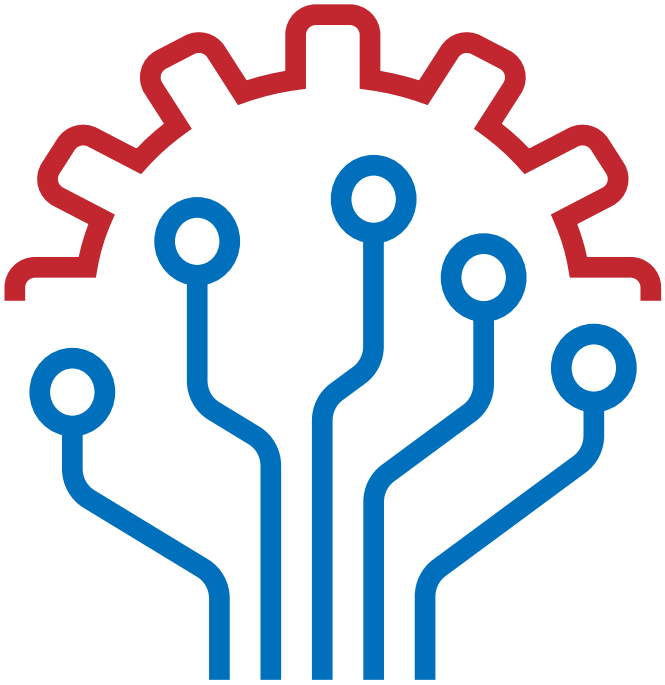
L'INTELLIGENCE ARTIFICIELLE AU SERVICE DE LA DÉFENSE



« Nous choisissons la voie de la responsabilité, celle de protéger à la fois nos valeurs et nos concitoyens, tout en embrassant les opportunités fabuleuses qui sont offertes par l'intelligence artificielle. »

Florence PARLY

Rapport de la Task Force IA
Septembre 2019

Liberté • Égalité • Fraternité
RÉPUBLIQUE FRANÇAISE

MINISTÈRE
DES ARMÉES

TABLE DES MATIÈRES

INTRODUCTION

Concept né en 1956, l'intelligence artificielle (IA) est désormais une réalité qui touche un très large public. Les progrès algorithmiques récents de l'apprentissage profond, combinés à l'explosion des volumes de données disponibles, ouvrent la voie à de multiples usages de l'IA, susceptibles de modifier en profondeur nos économies, nos modes de travail, mais également les équilibres stratégiques mondiaux.

Certains y voient une source immense de progrès pour l'humanité permettant de dégager l'homme des tâches fastidieuses, d'augmenter ses capacités cognitives, d'améliorer sa santé et son accès à la connaissance. D'autres, au contraire, n'entrevoient que les menaces que ces technologies font d'ores et déjà peser sur nos démocraties, sur notre vie privée et celles qu'elles pourraient faire peser demain sur nos emplois ou le respect de nos valeurs éthiques.

Entre immortalité, transhumanisme et fin du monde annoncé par le règne des robots, l'intelligence artificielle est aujourd'hui l'objet de tous les espoirs, les craintes et parfois les fantasmes.

Elle est aussi l'objet d'une compétition planétaire de grande intensité : grandes puissances comme entreprises privées, dont certaines ont atteint un poids économique considérable, annoncent chaque semaine de nouveaux résultats et de nouveaux investissements massifs dans le domaine de l'IA. La course aux talents est également lancée et si l'excellence de la formation scientifique française y est reconnue, elle ne bénéficie pas toujours suffisamment à notre pays ou nos entreprises. **Dans cette course, l'enjeu et le rythme sont tels que tout décrochage serait irrémédiable.**

Si les technologies d'IA joueront un rôle de premier plan dans la supériorité opérationnelle future, elles ne constituent pas, pour autant, une fin en soi pour les armées mais bien un moyen de continuer à remplir ses missions : garantir à la France, aujourd'hui et demain, sa capacité à assumer ses responsabilités pour la paix et la sécurité dans le monde, assurer la protection de son territoire national, de ses concitoyens et de ses intérêts, tout en agissant dans le strict respect du droit international humanitaire et sans exposer inutilement la vie de ses soldats.

Les armées françaises ne sauraient donc se tenir à l'écart de ces développements, sous peine de manquer un tournant technologique majeur et de perdre la supériorité opérationnelle qui est la leur aujourd'hui. Dans le cadre de la stratégie nationale voulue par le Président de la République, ce document constitue la stratégie du ministère des armées en matière d'IA. Il présente une feuille de route ambitieuse, pragmatique et respectueuse des valeurs de notre pays, qui permettra à l'ensemble du ministère, forces comme administrations et services de soutien, de bénéficier des avancées significatives de cette technologie si prometteuse.

L'INTELLIGENCE ARTIFICIELLE ET LA DÉFENSE

ÉTAT DES LIEUX D'UNE RÉVOLUTION

1- Un domaine en plein essor

Terme très vendeur mais jugé impropre par de nombreux experts, car attribuant à des machines des caractéristiques propres à l'être humain, l'intelligence artificielle recouvre des notions diverses et évolutives dans le temps qu'il convient de préciser.

Le Journal Officiel définit l'intelligence artificielle[1] comme le « ***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*** ». En cela, l'IA possède une frontière mouvante, au gré des progrès scientifiques et de la perception humaine des tâches dites « intelligentes » : ainsi il y a plus de 30 ans, les premières démonstrations de théorème en géométrie réalisées par des ordinateurs, les premiers systèmes de dialogue homme-machine étaient considérés comme à la pointe de l'IA. Aujourd'hui, nous les voyons comme des algorithmes classiques utilisant sans finesse la puissance de calcul informatique.

Quel qu'en soit le périmètre, l'IA reste un moyen et non une finalité en soi : elle n'est pas un substituant à l'homme, quand bien même elle effectuerait certaines tâches pour lui.

Plus concrètement, l'intelligence artificielle est utilisée dans les applications où il s'agit :

- ***de détecter*** et ***reconnaître*** des données (texte, voix, images, vidéos, ...) voire de ***prédire*** des données futures ;

- ***de rechercher des corrélations*** entre des données pour en déduire un comportement générique ou au contraire lever une alerte en cas de comportement anormal ;

  - d'***optimiser*** des problèmes à forte combinatoire comme des flux logistiques ou des

1 Vocabulaire de l'intelligence artificielle. JORF n°0285 du 9 décembre 2018, texte n°58.

trajectoires d'aéronef ;

- de ***raisonner*** sur des données symboliques pour ***déduire*** ou pour ***diagnostiquer***.

Du point de vue technique, l'intelligence artificielle comprend deux branches majoritaires : les ***approches symboliques*** basées sur le raisonnement (systèmes à base de règles) et les ***approches connexionnistes*** plus proches de l'empirisme, fondées sur l'apprentissage à partir de grandes bases de données (réseaux de neurones).

Les progrès de la dernière décennie — traitement de données massives, algorithmes utilisant les réseaux de neurones profonds, capacité de calculs et utilisation des GPU (*Graphics Processing Unit*) — ont eu un effet d'entraînement et de redécouverte des différentes techniques de l'intelligence artificielle. Ces effets ont été décuplés par la démarche de partage des algorithmes en source ouverte, ainsi que par les différents challenges de recherche qui ont permis de quantifier des progrès spectaculaires dans le domaine de la reconnaissance d'objets ou de la navigation autonome.

Figure 1 – Estimation par Gardner et PwC de l'évolution des niveaux d'autonomie pour le véhicule (sur la base d'études réalisées en 2017).

Cependant, en dépit de ces progrès indéniables, les technologies d'IA restent encore peu robustes à des environnements inconnus, difficilement généralisables. Leurs résultats sont parfois peu explicables ou mènent à des erreurs grossières. Ceci explique que l'emploi de l'IA reste aujourd'hui majoritairement cantonné à des tâches élémentaires ou peu critiques. Dans le domaine de la défense, l'emploi de l'IA nécessitera donc que ces technologies progressent pour en permettre un usage maîtrisé.

2- Dualité et spécificités militaires

Si le grand public a été frappé par le succès d'Alphago ou les prouesses sportives des robots de Boston Dynamics, aujourd'hui l'intelligence artificielle peine encore à se généraliser dans des applications industrielles et commerciales concrètes. Les secteurs du commerce électronique, du marketing, de la finance, de la maintenance industrielle ou des ressources humaines ont été les plus véloces à s'approprier ces technologies aujourd'hui en plein essor. Pour les particuliers, les premières applications sur des données non structurées (traitement de la parole et traitement d'images) envahissent les enceintes domestiques ou les smartphones. Le secteur de la santé a également fait l'objet d'avancées très significatives en analyse d'images de tumeurs pour atteindre des niveaux de reconnaissance supérieurs aux meilleurs professionnels entraînés.

Ces réalisations proviennent essentiellement des grands industriels du numérique, surtout américains et chinois, ayant accès au carburant de l'IA que sont les données massives fournies gratuitement par leurs clients à chaque interaction. Ayant initialement cherché à enrichir leurs produits et services par une meilleure connaissance de leurs clients, ils font désormais preuve d'ambitions plus vastes (véhicules sans chauffeurs, ***smart cities***, médecine personnalisée…), grâce à des moyens financiers considérables. Leurs produits font référence et l'étendue des cas d'usage qu'ils développent les rend attractifs pour le secteur militaire, notamment dans les nombreux domaines duaux. Comme dans le numérique en général, le secteur défense n'avance plus nécessairement en éclaireur, mais doit bénéficier des avancées du secteur civil et les adapter à ses usages particuliers lorsque c'est nécessaire.

Les armées doivent ainsi trouver le bon équilibre entre le bénéfice de ce qu'offrent les grands groupes numériques privés et souvent étrangers sans en devenir dépendantes, tout en développant de manière souveraine des applications spécifiquement militaires. Dans les applications les moins spécifiques et notamment dans l'optimisation de sa gestion administrative, des outils de consolidation financière ou de gestion des ressources humaines, les données et les besoins du ministère des Armées sont similaires à ceux d'un autre ministère ou d'une grande entreprise. Le marché civil développe et propose déjà des offres répondant à ces usages.

Pour les systèmes opérationnels militaires en revanche, il existe des spécificités importantes, que ce soit en termes de tâches à réaliser, de nature des données à manipuler (images infrarouge, données radar ou sonar…) ou d'exigence de performance et de robustesse. Les acteurs civils ne développent pas de traitement pour ces types de données militaires.

De plus, les systèmes opérationnels militaires présentent des caractéristiques que l'on rencontre peu dans le monde civil, à l'exception de certains systèmes critiques (aéronautique, systèmes bancaires…) :

- ces systèmes sont souvent **embarqués et déployés en milieu ouvert et inconnu ;**

- ils doivent répondre à des **exigences élevées en termes de latence et de robustesse,** mais disposent généralement de **faibles ressources en énergie** et de liaisons à débit limité entre eux ou avec des *data centers* ;

- une **qualification préalable** à leur mise en service sera systématique pour s'assurer de leur comportement.

Pour traiter ces spécificités, le ministère s'appuiera en grande partie sur le socle algorithmique existant et très majoritairement disponible en source ouverte, sauf cas particuliers où les risques de rétro-conception feraient l'objet d'une attention particulière. En revanche, plus les cas d'usage ou les données traitées seront spécifiques au domaine militaire, plus le ministère devra investir en autonomie dans la conception des chaînes algorithmiques et leur paramétrage.

3 - Des potentialités foisonnantes au service de la supériorité opérationnelle

Profitant de cette dynamique, les applications militaires de l'IA se développent, intégrant notamment la vision par ordinateur, la robotique intelligente, l'intelligence distribuée, le traitement automatique des langues ainsi que l'analyse sémantique et le croisement de données.

Le stratège et le chef militaire, dans leurs responsabilités opérationnelles et organisationnelles, doivent pouvoir tirer parti de l'IA et en faire un facteur décisif de supériorité opérationnelle. Il s'agit notamment de gagner en vélocité, en marge de manœuvre par une meilleure reconnaissance/détection des cibles et des dangers de terrains jusque-là inconnus, par des actions plus rapides et mieux ciblées, ainsi que par des actions de « déception » tout en garantissant le respect des lois de la guerre.

4- Mieux comprendre, anticiper toujours, décider plus vite

L'IA favorise un nouveau mode de traitement des données qui conjugue rapidité d'exploitation et analyse croisée et massive ; elle permet ainsi de dégager les grandes tendances et les singularités, bien au-delà et bien plus rapidement qu'un traitement humain. On peut donc s'attendre à ce que l'IA apporte une compréhension plus complète et plus rapide des situations dans des espaces opérationnels de plus en plus complexes et interdépendants.

L'IA permettra une meilleure anticipation des manœuvres de l'adversaire et une optimisation des processus opérationnels (orientation, recherche, exploitation et diffusion du renseignement). Bien calibrée, elle procurera de nombreux atouts, par exemple dans l'évaluation de la menace et l'optimisation de son traitement pour y faire face.

Le gain de temps dans l'accès et le traitement des données autorisé par l'IA va permettre d'élargir le champ d'exploration des hypothèses envisagées en planification et conduite des opérations. C'est notamment dans le domaine des signaux faibles, qui peuvent être précurseurs de changements importants, que l'apport de l'IA sera décisif, contribuant ainsi à réduire significativement l'effet de surprise. Les données issues du RETEX et traitées par l'IA seront également intégrées dans le processus décisionnel et viendront l'enrichir de manière itérative.

La meilleure compréhension de la situation apportée par l'IA va permettre de valider plus rapidement des hypothèses de modes d'action et donc de favoriser l'accélération du tempo décisionnel.

L'IA a donc la capacité, à court terme, de conférer aux processus décisionnels des armées la supériorité opérationnelle nécessaire pour prendre l'ascendant sur de nombreux types d'adversaires.

5 - Mieux protéger le soldat

Au-delà de la conduite des opérations, l'IA bénéficiera aux militaires eux-mêmes. Par un traitement massif des données de santé et un élargissement de la veille sanitaire, l'IA identifiera des facteurs de risques liés aux environnements et aux conditions d'emploi des forces, et proposera les mesures de protection adaptées pour limiter l'impact sur la santé des militaires.

Intégrée à la simulation, l'IA permettra également d'améliorer l'entraînement des unités et la formation différenciée des individus, en particulier lorsqu'elle sera associée à la réalité augmentée, dans le cadre de *war gaming*, de « jeux sérieux » ou encore en environnements virtuels immersifs.

La robotique autorisera pour sa part une plus grande mise à distance du soldat et une meilleure autoprotection. Ce sera le cas, par exemple, pour les interventions en milieu contaminé, la lutte contre les incendies, le déminage terrestre ou sous-marin, ou encore la lutte contre les essaims de drones.

Enfin, l'amélioration de la protection du combattant permise par l'IA n'est pas uniquement cantonnée au domaine opérationnel puisque l'IA apportera également une aide significative en faveur du respect des valeurs du DIH. En permettant une meilleure appréciation de l'environnement des opérations à un niveau tactique, opératif et stratégique, l'IA contribuera fortement à :

- améliorer la discrimination entre combattants et non combattants ;

- renforcer la proportionnalité en maîtrisant les effets des armes, en fonction de la menace ;

- garantir une action déterminée par la stricte nécessité.

Ainsi, contrairement à certaines idées reçues, l'IA recèle un potentiel qui, bien encadré et maîtrisé, conduit à une meilleure prise en compte par les armées françaises des principes fondamentaux du droit des conflits armés.

6- Libérer l'homme des tâches ancillaires

Outre les optimisations évoquées ci-dessus, l'intelligence artificielle est annonciatrice d'une profonde transformation dans la préparation et la conduite des opérations. L'IA doit à terme prendre en charge de nombreuses actions ancillaires et répétitives. En libérant ainsi l'homme de ces tâches particulièrement chronophages, elle lui permettra de se concentrer sur celles à haute valeur ajoutée. Dans la chaîne de commandement notamment, l'IA permettra aux états-majors de se concentrer sur la réflexion et la prise de décision.

Dans le domaine de l'observation spatiale, les interprètes d'image pourront exploiter efficacement le flux d'informations, largement supérieur avec les satellites CSO à celui de la génération précédente. En opérations, des systèmes munis d'IA pourront remplir les fonctions d'équipiers au profit des combattants : par exemple, les avions pilotés pourront être accompagnés de drones équipiers destinés à les appuyer dans leurs différentes missions.

Par ailleurs, il est communément admis que 80% des erreurs humaines surviennent lors des tâches routinières. En les faisant exécuter par de l'IA, le risque d'erreur humaine liée à la répétitivité et à des actions mécaniques s'en trouvera réduit.

7- Optimiser les flux et les ressources

L'intelligence artificielle permet d'implémenter des modèles prédictifs qui permettront de prévoir et d'optimiser les flux logistiques du ministère, la gestion technique de flottes de matériels et l'ordonnancement des opérations de maintenance associées, les engagements financiers ou encore les opérations de recrutement. L'optimisation des flux et des ressources par l'analyse prévisionnelle est une application particulièrement mature de l'IA, qui comporte de plus une forte dualité. Par conséquent, même en tenant compte des spécificités propres aux opérations militaires, l'IA pourra rapidement apporter des gains significatifs dans ce type d'applications, comme en témoignent les développements du « Lab BI » du SGA.

8- Une révolution qui n'est pas exempte de menaces et de risques

Parce que l'IA innervera tous les systèmes, les menaces liées à l'usage de l'IA sont les contreparties de ses opportunités et pourraient impacter tous les domaines d'intérêt : renseignement, commandement, engagement, maintenance et soutien, condition du personnel (moral des soldats…).

Aujourd'hui les technologies d'IA n'ont pas atteint une maturité capable de bouleverser les rapports de force et changer la nature de la guerre. Mais ce domaine évolue rapidement et son coût technologique décroît sans cesse, ce qui laisse entrevoir à court terme de nouveaux modes d'action et des ruptures d'emploi ou de seuil. Ces nouvelles menaces se feront rapidement beaucoup plus prégnantes car aisément accessibles, notamment du fait du détournement de technologies commerciales ou de l'utilisation de robots « *low cost* ».

Elles font craindre en particulier :

- la prévisibilité de nos modes d'action par les IA adverses, et la perte de l'effet de surprise ;

- la paralysie de nos capacités de commandement par la neutralisation, le leurrage ou le détournement de nos technologies ;

- l'extension des opérations d'influence et des actions dans le champ informationnel (détournement de flux d'informations, décrédibilisation médiatique, *fake news*, etc.) ;

- le changement d'échelle et la multiplication des actions hostiles « à haute-fréquence » dans le domaine cyber (attaques coordonnées, actions de déception…).

9 - Compétition, nivellement et rupture

L'IA peut constituer un agent déstabilisateur des équilibres établis en favorisant la compétition en matière d'armement, susceptible d'aboutir à des ruptures technologiques ou au nivellement des positions stratégiques.

La course technologique engagée dans l'IA s'intègre dans la course aux armements qui est désormais relancée. Ce phénomène devrait être amplifié par la dualité et l'extension des applications technologiques de l'IA. Le champ des applications futures de l'IA étant très vaste, la plupart des États perçoivent que la hiérarchie établie de la puissance militaire peut être

modifiée à leur avantage. Sans nécessairement être en pointe sur l'ensemble du spectre technologique de l'IA, la maîtrise de quelques technologies-clés peut suffire à bousculer l'ordre établi.

De fait, l'IA peut niveler les positions stratégiques, notamment dans un cadre d'emploi asymétrique. Ainsi, des acteurs non-étatiques peuvent adroitement exploiter de futures technologies civiles sur étagère pour élaborer des surprises tactiques à partir de moyens inédits. À l'échelle des États, certains peuvent miser sur les technologies de l'IA offrant de nouveaux leviers de déstabilisation, par exemple en matière d'attaque cyber ou de désinformation (logiciel de manipulation audio, vidéos « augmentées » par l'IA – ***deepfake*** – ou encore logiciel d'analyse comportementale de groupes d'opinion…). La démarcation entre réalité et fiction risque de s'estomper ce qui pourrait affaiblir le crédit politique des démocraties.

Le domaine de l'IA se prête également à des évolutions incrémentales rapides qui peuvent déboucher sur des ruptures technologiques.

Des progrès tangibles devraient ainsi intervenir dans les domaines de la détection, de l'agression ou de la prise de décision, favorisant de nouveaux déséquilibres propices à des scénarios d'escalade. Par exemple, de tels scénarios d'escalade pourraient provenir :

- de la peur de subir une « surprise technologique » ;

- de la tentation de frapper en premier (frappe préemptive ou préventive) ;

- de la célérité des progrès technologiques qui ne donne pas le temps politique pour s'accorder sur des mesures de confiance dans le domaine de la maîtrise des armements.

10 - Risques induits par l'utilisation de l'IA

Le déploiement de l'intelligence artificielle n'en est qu'à ses débuts et se limite encore souvent à des cas d'usage plutôt tolérants aux erreurs. Le passage à l'échelle industrielle, notamment pour l'IA militaire, implique des exigences renforcées en termes de robustesse. La technologie progresse rapidement mais il y a des risques inhérents à certaines techniques : ainsi les réseaux de neurones profonds peuvent encore être manipulés pour leurrer la perception humaine, par exemple en introduisant dans deux images des différences imperceptibles pour l'œil humain.

De même, les techniques d'apprentissage présentent différents risques :

- de biais involontaires en particulier lorsque les données d'apprentissage ne sont pas représentatives (par exemple, biais ethnique dans des données de population) ;

- de biais volontaires si un tiers a pu modifier les données d'apprentissage ou le modèle afin de produire un résultat anormal éventuellement sur demande ;

- de reconstitution de données particulièrement sensibles d'apprentissage (rétro-conception), en particulier si le tiers dispose de connaissances sur les techniques ou les outils d'apprentissage ayant été utilisés ;

- de résultats opaques ou peu explicables auxquels il sera difficile pour l'homme de faire confiance dans des systèmes critiques.

D'une manière générale, la qualité des données d'apprentissage est déterminante pour acquérir des algorithmes robustes. Ainsi, si les données d'apprentissage sont inexistantes, inaccessibles, en quantité insuffisante ou sans correspondance avec le cadre d'emploi souhaité, les résultats obtenus ne seront pas satisfaisants.

Enfin le risque de dépendance à une technologie qui simplifie l'utilisation de certains outils ne doit pas être écarté. Par conséquent, le maintien des compétences permettant de réaliser une mission de façon résiliente et avec un recours à l'IA réduit devra être recherché. Le déploiement de l'intelligence artificielle devra ainsi s'accompagner des mesures nécessaires pour éviter une perte de compétence humaine qui rendrait difficile la réalisation de mission en l'absence de ces traitements.

Si certains risques liés à l'emploi de l'IA ne lui sont pas spécifiques (leurrage, porte dérobée, rétro-conception, faible résilience…), leur mise en œuvre peut les rendre moins détectables car moins « intuitifs ». Les risques liés à l'emploi de l'IA et les moyens de s'en prémunir font l'objet de recherches en plein essor qui devront être suivies avec attention et soutenues par le ministère des Armées.

UN PAYSAGE INTERNATIONAL QUI REFLÈTE LES GRANDES TENSIONS DU MONDE

11 - Une compétition internationale déjà lancée

Récemment, de nombreux pays ont diffusé des stratégies civiles en matière d'intelligence artificielle. Cette accélération et l'effet d'émulation mondiale qui l'accompagne témoignent du sentiment partagé que la maîtrise de l'IA représente un facteur de puissance incontournable à l'avenir. Les différentes stratégies IA publiées récemment révèlent une hiérarchie mondiale de la puissance IA qui peut s'envisager de la manière suivante :

- deux « superpuissances » : États-Unis et Chine, hors d'atteinte par les autres, contrôlant une immense masse de données, disposant d'un écosystème articulé autour d'entreprises intégratrices puissantes à vocation mondiale (GAFA[2] et BATX[3]) et pouvant encore démultiplier leur domination grâce à leurs moyens scientifiques et financiers ;

- une puissance intermédiaire en devenir : l'UE, dont le positionnement strict sur les questions juridico-éthiques pourra constituer une force comme une faiblesse selon son impact (puissance normative agrégeant de nombreux acteurs étatiques ou privés *vs*. risque de définir une politique de recherche ou de développement entrepreneurial trop timorée ou entravée par des règlementations trop contraignantes) ;

- un second cercle d'États : on y trouve notamment la France, l'Allemagne, le Royaume-Uni, le Japon, la Corée du sud, Singapour, Israël et le Canada. Ils disposent de certains atouts mais sans masse critique suffisante. Leur degré d'autonomie dépendra des effets de levier obtenus grâce aux coopérations qu'ils sauront établir, et de la pertinence des stratégies de niches maximisant leurs avantages comparatifs.

Figure 2 – Historique des publications de stratégies IA nationales.

12 - Des stratégies à l'image des ambitions nationales

a) Un socle commun indispensable : conquête des talents, effort de recherche, pouvoir normatif

Parmi les points communs de ces diverses stratégies figurent en premier lieu la préservation des talents nationaux et la captation des compétences extérieures. Toutes souhaitent développer un effort important de recherche, fondamentale ou appliquée, et décloisonner les applications de l'IA. Les briques technologiques doivent ainsi diffuser du secteur privé vers le secteur public, du domaine civil au militaire, entre le monde de la recherche et celui de l'industrie, et enfin entre les différents métiers de l'IA (complémentarité[4]). Cette préoccupation se traduit dans les stratégies organisationnelles, visant notamment à créer les structures facilitant ces irrigations croisées.

Par ailleurs, tous les États souhaitent jouer un rôle actif, et si possible moteur, dans l'élaboration des normes de l'IA. En effet, la production de standards mondiaux permet d'apparaître comme une puissance contribuant à façonner un socle IA encore en évolution (normes technologiques, juridiques, commerciales, comportementales).

b) Des divergences majeures autour de l'emploi : aspects éthiques et sécuritaires

Les divergences relevées touchent tout d'abord le volet éthique. On peut ainsi distinguer des acteurs peu concernés par ces questions et d'autres plus scrupuleux.

Les deux grands acteurs, les États-Unis et la Chine, présentent une différence de fond. La Chine peut en effet disposer d'une capacité de pilotage plus ferme des acteurs privés et leur prescrire de coopérer avec la sphère publique, y compris militaire. La Chine a ainsi élaboré le principe de « *civil-military fusion* » visant

2. Google, Apple, Facebook et Amazon.
3. Baidu, Alibaba, Tencent et Xiaomi.
4. Par-exemple, certains GAFA, en tant que grands consommateurs d'énergie, investissent significativement pour développer des modes de consommation d'énergie « intelligents ».

à maximiser les transferts entre les différents pôles (recherche, industrie, État, armées). Le modèle chinois étend résolument les applications de l'IA au domaine sécuritaire. Les relations sont plus compliquées aux États-Unis où les réticences de certaines entreprises à collaborer avec le ***Department of Defense*** ont déjà perturbé certains projets (exemple du projet ***Maven***[5]). Ces aspects socio-institutionnels constituent la principale distinction entre la Chine et les États-Unis.

c) Une compétition agressive inscrite dans le moyen terme

La compétition pour acquérir les ressources nécessaires au développement de l'IA est donc déjà amorcée et elle devrait s'accentuer. Ces ressources sont autant immatérielles (capter des compétences rares en matière de ressources humaines) que matérielles (capter des technologies-clés, etc.).

13 - Une réflexion éthique accaparée par les « robots-tueurs »

Le développement technologique s'accompagne chez tous les acteurs d'une prise de conscience des implications de l'IA en termes éthiques. Les différents échanges au niveau international ont cependant tendance à se focaliser sur le potentiel développement de systèmes d'armes létaux autonomes (SALA). Un Groupe d'Experts Gouvernementaux (GGE) dédié a ainsi été mis en place au sein de la Convention sur Certaines Armes Classiques (CCAC) depuis 2017.

Les États sont fortement divisés sur les résultats à atteindre dans ce cadre. La France contribue activement au débat en défendant une position « réaliste » : les SALA n'existent pas à ce jour et une interdiction préventive ne permettrait pas de répondre aux défis juridiques et éthiques posés par ces systèmes.

PRINCIPES DIRECTEURS POUR UNE IA DE DÉFENSE MAÎTRISÉE

15 - Conserver notre liberté d'action et l'interopérabilité avec nos alliés

Pour maintenir leur supériorité face à des adversaires de plus en plus agiles dans la maîtrise des technologies numériques, les armées françaises doivent aujourd'hui anticiper les ruptures d'emploi qu'apporteront inévitablement les avancées technologiques liées à l'intelligence artificielle.

Son introduction dans les systèmes d'armes, les systèmes d'information et les systèmes de commandement est, dès à présent, un enjeu opérationnel majeur pour conserver l'ascendant face à des menaces tant symétriques qu'asymétriques, mais également pour rester au niveau des nations de premier rang en coalition.

Nos alliés dans un cadre national, OTAN ou UE sont eux-mêmes impliqués dans des processus d'intégration de l'IA dans leurs systèmes militaires. De fait, l'interopérabilité avec nos alliés doit être maintenue via des normes communes, indispensables à la conduite des opérations en coalition. Par ailleurs, la capacité à contrer les effets des IA adverses sera un facteur déterminant de domination stratégique, qui impose de se doter sans tarder des compétences et des technologies qui permettront de garder un ascendant

16 - S'appuyer sur une IA de confiance, maîtrisée et responsable

Par nature, les systèmes comportant de l'IA sont appelés à fonctionner avec une certaine autonomie. Pour autant il est indispensable pour le ministère des Armées de disposer de systèmes robustes, sécurisés permettant d'assister le soldat et le commandement en confiance, sans effet « boîte noire », tout en conservant la responsabilité humaine de l'action.

Cette IA de confiance repose notamment sur la rigueur de conception des systèmes qui doit garantir le total respect du cadre fixé par l'homme, ainsi que sur la capacité du ministère à évaluer et certifier ces systèmes.

L'homme pourra alors tirer le meilleur parti de son système et obtenir ainsi un réel facteur de supériorité opérationnelle. L'objectif est de combiner jugement humain et puissance des algorithmes pour décider et agir avec clairvoyance dans des tempos opérationnels toujours plus élevés.

La performance opérationnelle sera supérieure à celle de l'humain ou de la machine pris isolément, et même des deux juxtaposés.

17- Maintenir la résilience et l'évolutivité de nos systèmes

Dans un environnement où la réussite des engagements repose sur les réseaux de communication et l'accès à l'information, les questions de robustesse et de résilience sont essentielles. Les armées françaises doivent se doter des moyens garantissant ces qualités afin de toujours garantir la

5. Des salariés de Google se sont émus des possibilités que leurs travaux soient utilisés à des fins militaires (analyse d'imagerie militaire), signant une pétition pour boycotter le projet.

poursuite des objectifs opérationnels. L'intégration, robuste, de l'IA permettra de disposer de fonctions autonomes qui offriront des solutions pertinentes notamment en cas de limitation, neutralisation ou impossibilité des communications. Ceci nécessitera de valider et qualifier ces fonctions puis d'adapter le soutien pour le rendre cohérent des opérations en environnement très contesté.

Ces environnements conduiront d'ailleurs les systèmes dotés d'IA à devoir parfois fonctionner en mode dégradé. Il faudra alors que les unités opérationnelles soient en mesure d'utiliser ces systèmes dans ces modes et conservent la capacité à mener efficacement leurs missions avec un recours minimum à l'IA ; cela devra faire l'objet de formations et d'entraînements réguliers au profit des forces.

Une des caractéristiques principales de la conception et de l'acquisition des capacités militaires est de s'inscrire dans le long terme : de nombreux équipements ont une durée de vie qui dépasse 50 ans. Pour ce qui concerne l'IA, domaine fortement dual et dont le cycle d'évolution est beaucoup plus court, il est essentiel que les équipements en cours de conception intègrent au plus tôt des systèmes à base d'IA et conservent une possibilité d'évolution sur plusieurs décennies.

18 - Préserver un cœur de souveraineté

Comme le souligne la revue stratégique de défense et sécurité nationale « … ***la maîtrise de l'intelligence artificielle représentera un enjeu de souveraineté, dans un environnement industriel caractérisé par des innovations technologiques rapides et aujourd'hui dominé par des entreprises étrangères*** »[6].

L'écosystème mondial de l'intelligence artificielle est dominé par les grands acteurs du numérique américains et chinois qui développent des capacités internes et rachètent de nombreuses sociétés prometteuses. D'un côté se trouvent, les GAFA (Google, Apple, Facebook et Amazon), Microsoft et IBM et les écosystèmes de PME et startups spécialisées qui se sont développés majoritairement autour de San Francisco et de New-York. De l'autre, les BATX (Baidu, Alibaba, Tencent et Xiaomi) et de nombreuses startups créées principalement autour de Beijing et de Shenzhen donnent à la Chine un avantage certain.

L'intelligence artificielle nécessite également des capacités de calcul massif, par exemple dans le cas le plus répandu des technologies du « ***deep learning*** », pour entraîner des réseaux de neurones avec de grands jeux de données. Ces capacités sont généralement accessibles dans des ***clouds*** publics ou privés, lesquels sont là aussi majoritairement dominées par des acteurs américains (Amazon Web Services, Microsoft Azure, Google).

Dans ce contexte dominé par des acteurs privés ou étatiques étrangers, la France ne peut se résoudre à dépendre de technologies dont elle n'a pas la maîtrise. Dans le cas de l'IA militaire et afin d'assurer la confidentialité et la maitrise de nos informations, il est indispensable de maintenir notre souveraineté technologique.

Sur le plan de la recherche, la France est très bien placée au niveau mondial et souvent considérée comme la meilleure en Europe[7]. Pour autant, l'industrialisation et la déclinaison en services de l'IA est moins avancée qu'au Royaume-Uni, au Canada ou en Israël. Cette situation se vérifie aussi bien dans le secteur industriel civil que dans celui de la défense. Afin d'éviter un décrochage technologique dans le domaine de l'IA, il est donc essentiel d'évoluer vers un meilleur équilibre entre recherche fondamentale et applications industrielles, mais aussi de développer des avantages stratégiques comparatifs (stratégie agile de « niches » de supériorité, seul ou en collaboration).

En parallèle, il sera nécessaire d'organiser les moyens de stockage et de se doter des outils d'administration, de préparation et de valorisation dans le cadre d'une politique globale des données. En outre, pour des applications critiques telles que des systèmes d'armes, il sera indispensable de pouvoir auditer les caractéristiques des algorithmes et des données ayant éventuellement servi à l'apprentissage, mais également de disposer de capacités à les faire évoluer.

Si des algorithmes génériques sont à la disposition de tous, leur paramétrage, leurs éléments d'apprentissage, leurs combinaisons ainsi que les données sont, en revanche, soigneusement conservés par leurs concepteurs. Le maintien de la souveraineté numérique passe donc également par la maîtrise des algorithmes et de leur paramétrage, et par la gouvernance des données.

FEUILLE DE ROUTE DU MINISTÈRE DES ARMÉES

20 - Un cadre éthique et juridique robuste pour le ministère des Armées

Le ministère est particulièrement conscient des questions éthiques et juridiques que peut soulever l'usage de l'IA dans des applications de défense, que ce soit pour ses tâches administratives et tech-

6 *Revue stratégique de défense et de sécurité nationale*, p. 74, octobre 2017.

7 *Artificial Intelligence – A strategy for European startups*, Roland Berger, October 2018.

niques ou pour l'emploi opérationnel. L'éthique et le droit sont au cœur de la formation des militaires français. Les principes du droit international humanitaire (nécessité, humanité, proportionnalité, distinction), et les valeurs issues d'une riche tradition philosophique, historique et opérationnelle (courage, générosité, souci de l'autre, efficience, responsabilité et réalité) sont intégrés dans le processus rigoureux et séquencé de planification de l'usage de la force, et d'une chaîne de décision de l'emploi de la force établie par des règles d'engagement, validées par l'autorité politique.

Pour éviter que les technologies à base d'IA ne remettent en cause ces principes, en particulier la place de l'homme dans l'action militaire, leur développement pour des besoins de défense maintiendra systématiquement la responsabilité du commandement militaire dans l'emploi des armes. Ainsi, la France n'envisage pas de développer des systèmes pleinement autonomes, échappant totalement au contrôle humain dans la définition et l'exécution de sa mission. La France sera fidèle à ses engagements internationaux et continuera à contribuer de façon volontariste aux travaux en cours dans le cadre de la CCAC et plus particulièrement du GGE sur les technologies émergentes dans le domaine des systèmes d'armes létaux autonomes (SALA).

C'est pourquoi la ministre des Armées a décidé de doter le ministère d'un dispositif global qui nourrisse sa réflexion et alimente sa démarche éthique tout en la rendant transparente et explicite.

21 - Un comité d'éthique ministériel

Un comité ministériel d'**éthique** pluridisciplinaire et permanent, centré sur les technologies émergentes dans le domaine de la défense sera mis en place. Il veillera au respect dans la durée des principes **énoncés précédemment** et nourrira la réflexion ministérielle, alors que de nouveaux usages de l'IA émergent chaque jour. Ce comité, qui sera mis en place en 2019, échangera étroitement avec le Comité consultatif national d'éthique.

Sa composition, comprenant des personnalités qualifiées extérieures au ministère, répondra au nécessaire équilibre entre crédibilité et efficacité opérationnelle. Doté d'une capacité d'auto-saisine, ce comité rendra des avis consultatifs qui seront publics par défaut, sauf contrindication liée à la confidentialité des sujets traités.

➢ Mettre en place un comité ministériel d'éthique d'ici la fin de l'année 2019.

22 - Des mesures de sensibilisation aux usages de l'IA

Pour s'assurer que ceux qui auront à les mettre en œuvre, en mesurent bien les tenants et aboutissants, une phase de formation et d'entraînement sera instaurée avant l'emploi opérationnel des systèmes intégrant des fonctions d'IA. Il s'agit de sensibiliser individuellement l'ensemble du personnel aux atouts mais aussi aux risques induits par cette technologie. Tous seront sensibilisés à la valorisation de la donnée.

➢ Mettre en place des actions de sensibilisation à l'utilisation de l'IA, plus particulièrement du point de vue de l'éthique, auprès des personnels du ministère.

23 - Des mesures techniques pour une IA de confiance

L'IA reste une technologie jeune et parfois peu mature qui peut produire des résultats aberrants pour la perception humaine. Par exemple, des reconnaissances d'images — reposant sur un apprentissage statistique et l'utilisation de réseaux de neurones profonds — peuvent produire un résultat totalement erroné[8] ou se faire leurrer par la variation de quelques pixels.

Ces erreurs peuvent résulter de diverses causes :

- erreurs d'implémentation provenant de données d'apprentissage contextualisées mais non représentatives de l'ensemble de la population ;
- dysfonctionnement des algorithmes développés, ce qui nécessite de pouvoir les expertiser avant mise en service ;
- comportement insuffisamment maîtrisé des solutions matérielles ou logicielles intégrées dans le système d'IA au regard de la criticité de la fonction.

Le ministère veillera à apprécier pour chaque application de l'IA un « juste niveau » de confiance et de robustesse exigible. Ce « juste niveau » est établi en fonction de la criticité des fonctions remplies et découle d'une analyse de risque systématiquement conduite dès la phase de conception. Cette analyse de risque doit permettre d'identifier parmi les différentes fonctions, celles qui seront les plus critiques pour en déduire des exigences en termes de développement, de qualification et de suivi en

8. À titre d'exemple, en juin 2015, l'application de reconnaissance d'images de Google a identifié deux personnes afro-américaines comme étant des gorilles. À l'été 2018, le logiciel de reconnaissance faciale Rekognition d'Amazon a alimenté une polémique en reconnaissant 28 criminels parmi les 535 membres du Congrès américain.

service.

La prise en compte des risques liés à l'intelligence artificielle dans les études de sécurité pourra conduire à ne retenir que certaines techniques, en fonction de la criticité de la fonction, ou à mettre en place une validation humaine obligatoire à certaines étapes de la chaîne de traitement algorithmique. Ces principes de conception d'une IA de confiance s'inscrivent dans le cadre éthique retenu par le ministère.

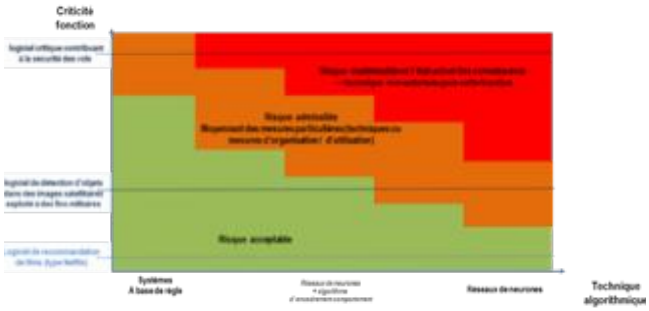


Figure 3 – Niveau de risque des technologies algorithmiques à base l'IA en fonction de la criticité.

À terme, la codification de certaines de ces exigences dans des normes simplifiera et homogénéisera les développements, permettant l'obtention d'une certification. Cette dernière, identifiée comme un axe d'effort nécessaire dans le rapport de Cédric Villani[9], constitue un objectif important. À l'avenir, la certification de certaines fonctions pourrait être effectuée par un prestataire de confiance, disposant d'une expertise reconnue et entretenue. Dans le cas de systèmes acquis à l'étranger, le niveau d'exigence sera comparable à celui exigé d'un fournisseur national.

➢ Intégrer la spécificité de l'IA dans les analyses de sûreté de fonctionnement des opérations d'armement et autres développements pour les besoins du ministère afin de déterminer le juste niveau de confiance nécessaire et de s'assurer du maintien d'un contrôle humain.

24 - L'indispensable construction de normes internationales

La normalisation est un élément important pour faire reconnaître des niveaux de performance et de qualité dans de nombreux secteurs. Le recours aux normes permet de simplifier la rédaction des cahiers des charges (une norme peut couvrir de très nombreuses exigences individuelles), mais également de positionner les industriels à l'export (la plupart des pays recourent à ces normes dans leurs propres contrats).

Bien qu'exprimées en termes d'exigences de performance, les normes ne sont toutefois pas totalement indépendantes des solutions techniques. Un haut niveau de performance ou des particularités dans la définition de la norme peuvent rendre difficile l'atteinte du niveau requis pour nos industriels ou demander de nouveaux travaux de conception et de développement. ***A contrario***, une norme trop peu exigeante ne permettra pas de distinguer les systèmes performants.

Dans le domaine de l'intelligence artificielle, les travaux de normalisation pourraient concerner la robustesse des algorithmes, les méthodes de préparation des bases d'apprentissage, les méthodes de développement et de test des modules logiciels intégrant de l'IA Une simple vérification de performance est insuffisante et il est nécessaire d'y ajouter des exigences sur le processus d'ingénierie logicielle. Cette méthode est déjà appliquée pour les logiciels critiques dans des secteurs tels que l'aéronautique, l'automobile, le nucléaire ou le ferroviaire. Néanmoins, la méthodologie et les normes actuelles concernant la sûreté de fonctionnement des logiciels critiques ne sont pas adaptées pour certaines familles techniques de l'IA comme les réseaux de neurones. Pour traiter ces sujets, un travail collaboratif entre les experts des logiciels critiques et les experts IA sera nécessaire.

Des travaux sur la rédaction de normes volontaires en intelligence artificielle ont débuté en 2018 via l'AFNOR qui a mis en place une commission nationale de normalisation sur les technologies d'IA[10]. Sur le plan international, de nombreux pays participent aux travaux de l'ISO, notamment les pays des deux premiers cercles de l'IA. À ce stade, les travaux concernent la définition d'un vocabulaire commun, d'architectures de systèmes et la mise en place d'un programme de travail. D'autres groupes de travail vont probablement se lancer dans les domaines qui mettent en place des normes et réglementations spécifiques comme l'aéronautique ou l'automobile.

➢ Participer activement aux travaux civils et militaires de normalisation et inciter les grands maîtres d'œuvres de défense à y être actifs au niveau national et international.

9. car « visant la confiance de toutes les parties prenantes dans leurs résultats [...] en termes de preuves théoriques à l'explicabilité, la transparence, la causalité et l'équité » (*cf.* rapport Donner du sens à l'IA : pour une stratégie nationale et européenne, p. 77).

10. via le lancement du sous-comité joint 42 de l'ISO et de l'IEC.

Le ministère des Armées doit également s'attacher à expliquer les enjeux de l'intégration de l'intelligence artificielle dans des systèmes critiques, y compris civils. Ces enjeux soulèvent en effet des questions éthiques, juridiques, d'industrialisation et de responsabilisation qui doivent être discutées avec nos partenaires.

➢ Diffuser la stratégie française en matière d'IA de défense et piloter sa mise en œuvre au niveau interministériel, comme dans les débats internationaux sur les systèmes critiques dotés d'IA.

25 - Données et hardware : le socle nécessaire au succès du développement de l'IA

Sur la base des principes exposés précédemment, le ministère décline une feuille de route à vocation opératoire pour le développement d'une IA adaptée aux besoins militaires. Elle repose en premier lieu sur une politique de gestion et de valorisation de la donnée et sur des capacités de calcul et de stockage.

La stratégie numérique du ministère[11] insiste sur l'enjeu des données qui concerne « ***le partage, l'exploitation et la valorisation des données*** à travers les nouvelles technologiques numériques » afin « ***de donner du sens aux masses de données collectées par les Armées*** ». La DGNUM met en place depuis 2018 une politique ministérielle de la donnée qui doit permettre :

- d'identifier les sources de données existantes en s'assurant de leur qualité et de leur complétude ;
- de mener des opérations de créations de corpus de données correctement annotées.
- d'organiser les moyens de stockage tout en se dotant des outils d'administration, de préparation et de valorisation des données ;
- de définir les modèles d'exploitation des données par l'analyse de cas d'usage en fonction des besoins des métiers : créer des bases de données dotées d'interfaces de partage normalisées et permettant la réalisation aisée de preuves de concepts et de travaux d'apprentissage.

La recherche de procédure de mise à disposition des données pour l'entraînement des algorithmes d'IA ou de test des algorithmes sur nos données réelles doit être conduite avec détermination. Elle sera une condition ***sine qua non*** à l'étude et à la compréhension des algorithmes, ainsi qu'à leur évaluation pour un emploi opérationnel.

26 - Gouverner la donnée

Accéder à des données fiables et à jour implique de maitriser le cycle de vie de la donnée, de sa captation à sa valorisation, en passant par sa production, son traitement ou sa conservation. Cette maîtrise constitue un enjeu majeur pour le ministère des Armées. Elle appelle à reconsidérer la donnée comme un actif stratégique et à mettre en œuvre une politique dont le principal axe d'effort repose sur la construction d'une véritable gouvernance des données.

La gouvernance des données a pour objectifs, d'une part, de se mettre en capacité de maîtriser le patrimoine dont dispose le ministère, d'autre part, de créer le cadre de confiance qui permettra de les partager dans le respect des exigences de conformité réglementaire, de sécurité et de bon usage. Elle doit au final garantir une exploitation optimale des données tout en allégeant la charge de saisie qui pèse sur les unités. À ce titre la gouvernance actuelle en silo, basée sur une vision urbanisée par métier doit évoluer vers une capacité transverse permettant l'échange de données entre systèmes référents et offrant une visibilité aux armées sur l'activité.

Des actions ont d'ores et déjà été lancées à trois niveaux :

- **stratégique, pour donner une vision cohérente des données**. Il s'agit de construire la carte des données ministérielles, d'identifier celles qui sont sensibles au regard des enjeux prioritaires, d'organiser les modalités de collecte, de définir les principes d'accessibilité et de piloter les politiques de mise en qualité ;
- **opérationnel, pour décliner le « code de la route » des données**. Il s'agit de poser et de mettre en œuvre les règles de partage propres à chaque type de donnée, de décliner les procédures d'échange entre producteurs, détenteurs et consommateurs, tout en assurant la traçabilité des données et leur bonne conservation. C'est une condition indispensable pour la rationalisation des saisies et des échanges en les SI, et un facteur de cohérence pour la construction d'indicateurs partagés ;
- **organisationnel, pour fixer les rôles et responsabilités**. Il s'agit d'identifier les acteurs intervenant dans le champ de la donnée,

11 ***Stratégie numérique du ministère des Armées***, DGNUM, avril 2018.

de définir les rôles et responsabilités et d'organiser la comitologie associée.

Cette gouvernance doit s'appuyer sur deux piliers :

- une architecture au service de la donnée qui doit permettre de stocker, collecter, traiter, exploiter, faire circuler les données, et de mettre à disposition de manière sécurisée ces capacités tant au profit des entités du ministère que dans une logique de partage avec des partenaires industriels de confiance.

  À terme, ARTEMIS permettra d'expérimenter l'ensemble de ces besoins. Dans l'intervalle, la plateforme d'ouverture, d'exposition et d'exploitation de données dite « POCEAD » permettra de mettre à disposition une première capacité technique de valorisation des données ainsi qu'une première brique méthodologique de gouvernance des données ;

- une véritable culture de la donnée en premier lieu pour sensibiliser l'ensemble des acteurs, sans se limiter aux seuls spécialistes. Il s'agit aussi de mieux appréhender les enjeux autour du bon usage des données et de l'exigence de transparence que cela implique, y compris la dimension éthique. Enfin, il s'agit d'anticiper les besoins en compétences sans lesquelles cette politique de la donnée ne peut fonctionner.

La montée en puissance dans la maîtrise de la donnée comme actif stratégique du ministère appelle un plan d'actions pluriannuel en trois temps :

- phase 1 (2018/2019) : construction d'une première capacité technique et méthodologique au service de la donnée, essentiellement à partir de POCEAD, fixant le cadre ministériel de gouvernance ainsi que les outils opérationnels permettant sa mise en œuvre ; détermination des niveaux de subsidiarité nécessaires au recueil, à la mise en qualité et à l'exploitation des données ;

- phase 2 (2020) : consolidation des capacités techniques et du socle méthodologique en s'appuyant sur les retours d'expérience issus de POCEAD et des cas d'usage expérimentés sur ARTEMIS ;

- phase 3 (2021) : maturité organisationnelle dans la maîtrise des données, en phase avec la mise en production d'ARTEMIS, et permettant de répondre aux enjeux stratégiques du ministère.

Cette politique devra aller de pair avec une révision des usages et des méthodes de conceptions des systèmes d'information futurs, notamment basée sur l'adoption d'architectures orientées données.

27 - Protéger les données personnelles

La distinction entre les données personnelles (qui permettent d'identifier une personne) et non personnelles est cardinale. La collecte et l'exploitation massive de données ne peut s'envisager que dans le strict respect de la législation en vigueur sur les données personnelles et notamment le Règlement Général sur la Protection des Données (RGPD).

28 - Anticiper la collecte et l'exploitation des données opérationnelles

Une démarche de collecte et de sauvegarde des données est un préalable à leur valorisation, mais également à des incréments successifs d'apprentissage. Il faut donc inclure dans nos différents systèmes des capacités d'enregistrement des données des capteurs. Certaines de ces données feront l'objet de traitements locaux à des fins d'apprentissage ou de tests. Ces enregistrements sont également un moyen de traçabilité en cas de dysfonctionnement.

Les applications faisant appel à la fusion et à la fouille de données réparties nécessitent également de disposer de capacités de télécommunication importantes afin de limiter les synthèses et fusions successives qui font perdre une partie de la richesse informationnelle des données brutes. Une fois le débit imposé, la répartition optimisée des traitements permettra d'exploiter au mieux les informations contenues dans les données échangées.

29 - Se doter de capacités de calcul et de stockage spécifiques

Au-delà des données, certaines applications utilisant de l'intelligence artificielle nécessitent l'accès à de très importantes capacités de stockage et de calcul. Le recours à l'informatique en nuage (*cloud*) est une des voies technologiques permettant de répondre à ces besoins.

Le *cloud* permet d'allouer selon les besoins des volumes importants de stockage très rapidement (ex : un Rafale produit 40 To/heure de données) ainsi que des ressources de calcul adaptées.

La technologie *cloud* augmente le niveau de résilience des infrastructures, grâce à une réallocation rapide et dynamique des ressources lorsque celles-ci sont défaillantes (ex : dans le cas d'une panne de disque dur ou d'une perte de serveur, possibilité de reconstruire les environnements au lieu de les réparer).

Le ***cloud*** apporte sécurité et fiabilité. L'automatisation des interventions et des déploiements de ressources via des scripts rendue possible par le ***cloud***, limite au strict minimum les interventions humaines et par conséquent les risques d'erreur ou les menaces associées.

Caractérisé par la standardisation et l'automatisation, le ***cloud*** est donc un moyen d'optimiser l'efficacité du ministère, en améliorant les outils collaboratifs ou encore en valorisant la donnée (saisie une fois, exploitée au besoin). C'est aussi un moyen essentiel pour faciliter les échanges avec l'environnement extérieur.

La stratégie ***Cloud*** du ministère des Armées s'inscrit pleinement dans le schéma en cercles de la stratégie ***Cloud*** de l'État :

- un ***cloud*** interne ou privé, dont l'accès est réservé au seul ministère, supportera l'appui direct aux opérations. L'exploitation en est assurée par la DIRISI ;
- un ***cloud*** dédié qui conciliera sécurité et usage des technologies innovantes et où les ressources seront également privatisées mais localisées chez un opérateur de confiance. Intégré à la structure cyberdéfense du ministère, il fera l'objet d'une stratégie industrielle spécifique avec des opérateurs de confiance et offrira un espace de partage collaboratif aux partenaires du ministère. À terme, il pourrait être susceptible de répondre aux besoins spécifiques d'autres organismes en quête d'un ***cloud*** sécurisé (autres ministères, BITD, OIV, etc.) ;
- un ***cloud*** externe ou public qui permettra de capter l'innovation en mettant à la disposition de tous des ressources partagées.

Les synergies prévues nativement entre les offres des différents cercles ***cloud*** vont faciliter la portabilité des codes d'un cercle ***cloud*** à un autre ainsi que l'accès à l'innovation présente sur Internet.

Enfin, la cybersécurité du ***cloud*** défense sera assurée par le ministère via la DIRISI et le CALID et conformément aux recommandations de l'ANSSI.

➢ Assurer par la mise en œuvre de la stratégie cloud du ministère, le stockage, la disponibilité et l'accès aux données au juste besoin, y compris classifiées, dans le respect des exigences de sécurité.

Enfin, d'autres technologies de rupture méritent d'être mentionnées car elles impacteront directement les performances et les capacités basées sur des mécanismes d'IA :

➢ S'impliquer dans la gouvernance des projets de calcul quantique et haute performance.

Axes d'efforts prioritaires pour le ministère

La combinaison et la convergence entre l'intelligence artificielle, la robotique, la réalité augmentée, la mise en réseau des systèmes, l'internet des objets, vont jouer un rôle central dans les systèmes de défense de demain et contribueront de façon significative à la supériorité opérationnelle. Au-delà d'une implémentation de l'IA dans les seuls systèmes opérationnels, les armées ont besoin de pouvoir plus largement exploiter l'IA dans leur dynamique de transformation numérique et explorer ses apports et ses implications potentielles dans toutes leurs activités.

Dans ce qui suit, les applications prometteuses sur le plan militaire ont été décomposées en 7 axes d'effort :

- aide à la décision en planification et en conduite,
- combat collaboratif,
- cyberdéfense et influence,
- logistique, soutien et maintien en condition opérationnelle,
- renseignement,
- robotique et autonomie,
- administration et santé.

Dans ces domaines, il s'agit de doter les armées de nouvelles capacités, c'est-à-dire des ensembles cohérents composés d'hommes et d'équipements, organisés, entraînés et soutenus selon une doctrine, en vue d'une finalité d'emploi opérationnel. Cette définition commune au sein des armées se résume sous l'acronyme DORESE (Doctrine, Organisation, Ressources-humaines, Équipements, Soutien, Entrainement).

Durant la présente LPM, il est déjà prévu à ce stade un investissement significatif de plus de 700 M€ en équipements et en études amont soit une moyenne annuelle d'un peu plus de 100 M€.

30- Aide à la décision et à la planification

Outre les données stockées, deux volets sont essentiels pour construire cet axe : un volet équipement (***infostructure***) qui permettra la fourniture d'un

socle de développement[12] d'applications métier et un **volet métier** qui permettra de développer des applicatifs (SI centré données). La compatibilité des applicatifs sera assurée au moyen d'interfaces standardisées (API[13]). La suite de ce paragraphe traite du volet métier lié à l'axe « aide à la décision en planification et en conduite ».

L'aide à la décision doit être disponible dans les centres de commandement (C2) de niveau stratégique, opératif et tactique, en amont (anticipation-planification) comme pendant la réalisation de la mission (conduite) et une fois celle-ci exécutée (évaluation). Elle nécessite le décloisonnement et le croisement des données car les outils de C2 manipuleront des données inaccessibles auparavant, issues de capteurs et de sources de natures très variées : renseignement, cyber, maintenance, santé, etc. Le traitement de données de masse basé sur l'apprentissage se fera majoritairement dans les data center dédiés. Une fois le module d'IA entraîné, il sera déployé vers les systèmes distants (opératifs, tactiques) via une transmission par les réseaux de télécommunications.

De manière très concrète, l'IA aidera à filtrer, valoriser, exploiter, partager les données, fournir des assistances pour aider à la manœuvre et ainsi offrir aux combattants des choix éclairés pour décider plus vite tout en réduisant l'incertitude (et en maintenant une décision humaine). Les interactions homme-machine bénéficieront des apports de l'IA : d'une part à travers des interfaces homme-machine augmentées, et d'autre part par une optimisation de la collaboration entre les unités, les systèmes et les combattants (dont coopération hommes/robots).

Aide à la décision en planification et en conduite

En phase de planification d'une opération pour un groupement tactique interarmes (GTIA), chaque véhicule ou groupe de véhicules se voit allouer une mission et un itinéraire recommandé en fonction de sa nature, de ses capacités de mobilité et d'action ou encore des menaces référencées sur la zone d'intervention.

Pendant l'opération, les véhicules peuvent disposer à tout instant d'une vue partagée de la situation tactique (cartographie mise à jour en temps réel), et ainsi synchroniser leur manœuvre. En se fondant sur leurs fonctions de perception, les véhicules peuvent par ailleurs déceler des changements dans l'environnement par rapport aux connaissances initiales et lancer une re-planification de la manœuvre initialement prévue. L'affectation ou la réaffectation de tâches, le calcul d'itinéraires, et les traitements automatiques permettant la détection des changements dans l'environnement sont des cas d'application typiques de la recherche opérationnelle en intelligence artificielle.

31 - Combat collaboratif

La coordination des systèmes et des entités opérationnelles est reconnue comme un facteur clé des opérations militaires dans tous les milieux afin d'accélérer le tempo de la manœuvre. Ainsi est né au début des années 2000 le concept de « combat collaboratif » pour bien signifier l'importance de mieux échanger, partager et exploiter les informations au niveau tactique. L'intelligence artificielle peut y contribuer tant sur l'exploitation des données pour l'anticipation, la réaction immédiate ou la conduite coordonnée de l'action, que sur la gestion intelligente des flux pour l'utilisation optimisée des débits accessibles.

Concernant l'exploitation des données, il s'agit notamment de partager l'information, de la fusionner, de la recouper pour améliorer la connaissance de la situation tactique. Il s'agit également d'améliorer le délai de réaction face aux menaces voire de préparer l'affectation des effecteurs et la répartition des tâches au sein des unités élémentaires.

Concernant la gestion des flux, l'intelligence artificielle pourra aider à sélectionner le meilleur compromis entre traitements centralisés et traitements décentralisés, à router de manière appropriée les différents flux, à faciliter l'interopérabilité entre systèmes hétérogènes et à prioriser les flux.

Combat collaboratif

Cas d'utilisation : Gestion des fréquences radio en opération et en coalition

Lors d'une opération terrestre en coalition, des sections de fantassins françaises, britanniques et allemandes sont chargées de sécuriser une zone géographique, par exemple en milieu urbain. Leurs communications transitent par des postes radios de nouvelle génération. Les fantassins communiquent entre eux via une onde nationale au sein d'une même section, ou via une onde de coalition entre nationalités différentes permettant les communications entre des postes radios issus de constructeurs différents. Avant l'opération, les fréquences radio ont été pré-affectées entre les nations de la coalition (planification du « spectre des fréquences »). Avec les réseaux intelligents, chaque poste radio, disposant de capacité d'analyse du spectre utilisable localement, pourra identifier de nouvelles ressources pour son

12 Ce socle sera fourni par ARTEMIS.

13 API : *Application programming Interface*.

propre usage : par exemple, si la section d'une nation partenaire opère momentanément en environnement deep indoor (galeries sous-terraines par exemple), elle pourrait potentiellement « libérer ses fréquences », qui deviendraient utilisables par les Français ou un autre partenaire.

32 - Cybersécurité et influence numérique

La cyberdéfense est un domaine d'application pour lequel l'IA aura vraisemblablement un impact opérationnel déterminant. Les applications prometteuses de l'intelligence artificielle sont les suivantes :

- l'analyse de traces dans un réseau à des fins de détection d'intrusion ou d'activité malveillante ;
- l'anticipation des menaces, en se basant sur les sources d'information disponibles (source ouverte) ;
- la mesure du niveau de résistance des systèmes ;
- la lutte dans le domaine de l'influence numérique.

Les travaux envisagés dans le courant de la LPM se focalisent sur le développement d'un écosystème propice à favoriser l'innovation en cycle court.

Dans ce but, la détection et l'anticipation des attaques s'appuieront sur la structure ARTEMIS qui permettra la captation et le traitement de la donnée par l'IA. Par ailleurs, ce sujet dual fera l'objet d'une coopération interministérielle (défi IA pour le cyber par exemple).

Le domaine de l'influence numérique bénéficiera quant à lui de synergies importantes avec le monde civil (ingénierie du marketing, lutte contre les opérations de désinformation, etc...).

Cyberdéfense et influence

Cas d'utilisation : Détection de cyberattaques

Une attaque informatique n'est pas nécessairement une action fulgurante mais plus généralement une opération phasée où peuvent s'écouler plusieurs semaines à plusieurs mois entre l'intrusion initiale et l'effet final (vol de données, sabotage...). La lutte contre les attaques informatiques repose sur une stratégie combinant des architectures robustes aux attaques (ce qui rend les actions de l'attaquant plus complexes, et donc le ralentit), à la capacité à détecter celles qui ont réussi avant que l'effet ne s'en fasse sentir. Pour cela, les données issues de l'activité des systèmes d'informations sont collectées par de nombreux capteurs disposés sur les réseaux, dans les terminaux et les serveurs, que l'activité soit habituelle (connexion d'utilisateurs, transmission de message, etc...) ou à risque (détection antivirale, identification de trafic réseau malveillant). Ces données, massives, sont exploitées au sein d'un « Security Operation Center ». L'intelligence artificielle permettra d'identifier à partir des données brutes ce qui relève d'un comportement normal ou d'un comportement caractéristique d'une attaque.

33 - Logistique et maintien en condition opérationnelle

L'IA appliquée à la logistique et à la maintenance constitue très certainement l'un des champs d'application les plus duaux. Les bénéfices de l'emploi de l'IA dans ces domaines peuvent s'envisager à court terme, car leur exploitation a déjà débuté dans le secteur civil. Elle offre des opportunités opérationnelles sur les axes suivants :

- augmentation de l'efficience de la chaîne logistique (*supply chain*) via la fluidification des flux de transport ;
- planification optimisée des actes de maintenance ;
- amélioration de la connaissance et de la gestion de la disponibilité des matériels grâce à la maintenance prédictive et l'optimisation de la maintenance préventive ;
- automatisation de certaines tâches (entreposage, maintenance, commandes, etc.) ;
- formation technique personnalisée

Dans le domaine aérien, le prochain standard F4 du Rafale commandé début 2019 disposera de traitements de maintenance afin d'améliorer la disponibilité de l'aéronef. Cette application de l'IA est en cours d'examen pour le prochain standard du MRTT dans la lignée des évolutions prévues pour les avions de gamme civile.

Logistique et maintien en condition opérationnelle

Cas d'utilisation : Maintenance différenciée et prévisionnelle

Les algorithmes d'IA permettront de mieux analyser les faits techniques et les données recueillies sur les systèmes ou sous-systèmes (via des capteurs), afin d'améliorer l'évaluation des risques de défaillance. L'analyse individuelle des équipements et des pièces élémentaires conduira à la mise en place d'opérations de maintenance différenciées.

Le cycle d'entretien ne sera plus global pour un même parc, mais un matériel sera soumis à un cy-

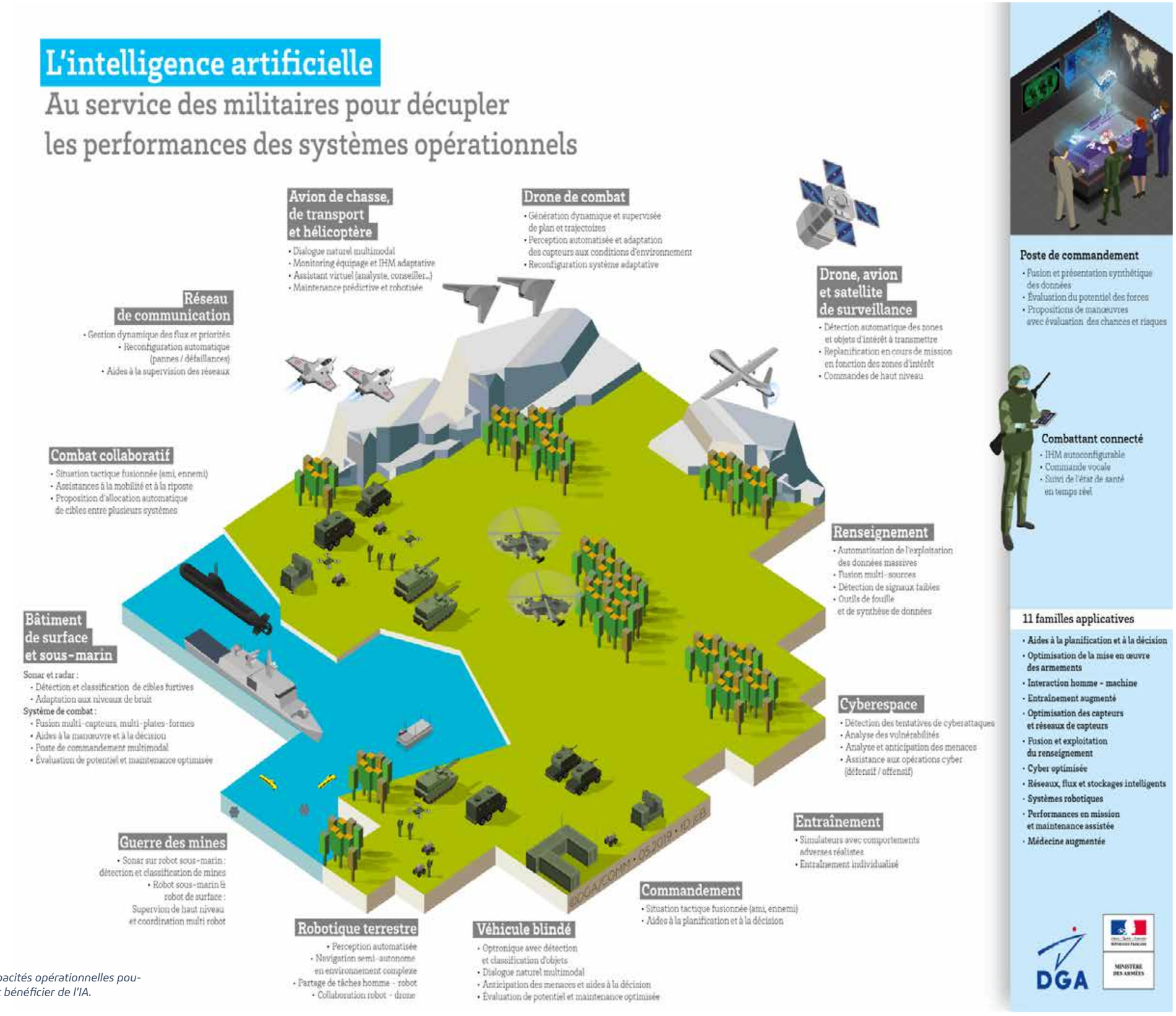


Figure 4 – Capacités opérationnelles pouvant bénéficier de l'IA.

cle de maintenance différent selon son utilisation réelle, l'usure des pièces pouvant être différentes selon le type d'usage. Les coûts de maintenance pourront donc être optimisés puisque certaines pièces seront remplacées moins souvent.

Les algorithmes d'IA permettront la mise en place d'alertes prédictives sur des équipements. Certaines opérations récurrentes ne devront plus être réalisées de manière systématique mais uniquement effectuées en cas d'alerte prédictive. Il sera également possible d'anticiper des risques d'avarie lourde sur certains systèmes ou sous-ensembles surveillés. Cette meilleure anticipation aura pour conséquence une meilleure planification des activités et des emplois des matériels.

34 - Renseignement

En matière de renseignement, la quantité de données à traiter ne cesse de croitre et l'enjeu consiste à les exploiter toujours mieux avec une ressource humaine comptée. Il s'agit donc d'utiliser l'intelligence artificielle pour automatiser les traitements et optimiser le croisement de données multi-domaines et multi-sources. L'objectif final est de recentrer le traitant sur les fonctions à haute valeur ajoutée.

Renseignement

Cas d'utilisation : Fouilles de données intelligentes

La lutte pour la supériorité informationnelle, nécessaire au succès des opérations, prend une nouvelle ampleur dans notre monde hyperconnecté où des informations d'intérêt sont noyées au milieu d'un flux d'échanges incessants et où les tentatives d'influence sont nombreuses. Afin de déceler au sein de ces quantités de données des évènements d'intérêt et extraire toute information pertinente sur les organisations adverses, l'analyste humain doit être secondé par des algorithmes d'intelligence artificielle pour :

· faire un premier filtre des données les plus pertinentes (« recommandation ») ;

· les prétraiter (traduction automatique, détection de personnes dans une image…) ;

· détecter des anomalies ou récurrences signatures d'activités suspectes ;

· recouper les informations publiques avec des sources militaires pour détecter des tentatives de désinformation.

35- Robotique et autonomie

En déportant à distance des moyens de perception et d'action, les robots et les drones permettent à l'humain d'éviter d'accomplir des tâches synthétisées par le sigle anglo-saxon «3D : ***Dull, Dirty & Dangerous*** ». Avec l'avènement de vecteurs et de capteurs plus compacts et grâce à des télécommunications performantes, les robots et drones sont d'ores et déjà déployés dans les armées notamment pour le déminage ou l'observation, même si la nécessité de les télé-opérer en permanence peut en limiter l'usage.

Dans le domaine terrestre, la robotique et l'amélioration des interfaces homme-machine sont des objectifs forts du programme SCORPION. Par exemple, des robots de type Mule disposant d'une fonction de suivi d'un leader humain seront disponibles à court terme. Robotique et autonomie

Cas d'utilisation : Coopération multi-robot, planification et affectation automatique des tâches aux différents systèmes

La coopération multi-robot vise à démultiplier les capacités d'action des systèmes robotisés dans tout type de missions. En phase de reconnaissance, un drone aérien peut jouer un rôle de capteur déporté afin d'augmenter la portée d'observation d'un robot terrestre, lui permettre d'anticiper les obstacles ou de s'infiltrer dans des recoins inaccessibles à la plate-forme terrestre. Dans le cadre d'une mission de surveillance, le recours à plusieurs robots mobiles coordonnés de manière automatique vise à assurer une meilleure couverture du site à surveiller, en réduisant en permanence les zones de masquage visuel tout en préservant une certaine imprévisibilité des rondes. En cas de suspicion d'intrusions multiples, les robots sentinelles peuvent également se répartir les points à inspecter afin de réagir plus rapidement. En outre, lors de la traversée d'une zone hostile, un essaim de drones a plus de chances de parvenir à son objectif qu'un robot unique, même si certains membres de l'essaim sont touchés. L'intelligence artificielle irrigue ces facultés de coopération multi-robot, à travers la planification et la coordination multi-agents, ainsi que la fusion de données d'observation. Quant à la coordination des mouvements au sein d'un essaim de drones, elle est souvent dérivée de techniques d'apprentissage automatique.

36 - Application aux soutiens

Le Secrétariat général pour l'administration a conduit des travaux prospectifs, en projetant les métiers administratifs à horizon 10 ans et en intégrant les technologies de l'IA (traitement et d'analyse de données, reconnaissance vocale, traitement du langage naturel, capteurs, robots logiciels…). C'est un défi culturel et organisationnel à relever pour lequel les axes d'effort suivants ont été identifiés :

- aide à la décision et analyse prédictive, pour établir des programmations, simulation ou optimisation de consommation de ressources (effectifs, masse salariale, budget et comptabilité, gestion des fluides) ;
- automatisation de tâches répétitives et chronophages avec des robots logiciels pour des processus à flux transactionnels (RH, contrôles en clôture de compte, traitement de factures) ;
- capteurs connectés dans les infrastructures, pour collecter des données automatiquement, faire du monitoring immobilier et de la maintenance prédictive ;
- agent ou usager « augmenté », avec des agents conversationnels (langage naturel et commande vocale) pour traiter des questions récurrentes, orienter, rechercher des informations pertinentes, et produire de manière automatisée des documents et suggestions à partir de contenus existants;
- nouveaux modèles de recrutement, avec automatisation de modes d'analyses issus des sciences comportementales et cognitives, prédiction de mobilités...

L'intelligence artificielle comporte des potentiels d'automatisation et de pilotage facilité. Les cas d'usage potentiels portent sur des thèmes transverses comme l'optimisation des processus, la gestion des relations avec les usagers (estimation des sollicitations, simulations, utilisation d'assistants virtuels pour épauler les agents publics ou directement interagir avec les usagers), le ciblage de contrôles régaliens et la détection automatique d'anomalies. Cette automatisation se fait au profit d'un recentrage sur le cœur des métiers administratifs et du service dispensé, en déchargeant ainsi les agents et les manageurs de tâches chronophages ou à moindre valeur ajoutée. Il s'agit de leur donner davantage de temps pour conseiller, produire des expertises ou prendre des décisions dans une logique de complémentarité homme-machine.

L'état-major des Armées a également conduit des travaux prospectifs dans le domaine de la santé. Ainsi, la collecte et le traitement par des outils dotés d'IA de données biométriques et médicales à l'entrainement et en opération permettra d'enrichir le soutien médical des militaires. Ces outils, embarqués ou non, pourront :

- bénéficier à la santé des militaires au quotidien, en aidant les personnels soignants dans leur diagnostic et l'accompagnement de la prise en charge ;
- optimiser la conduite des opérations, en apportant des informations pertinentes sur la gestion des personnels : état de fatigue, de stress, rotation des équipages ;
- permettre dans la durée l'identification de facteurs de risques ou de protection pour la santé des militaires.

GOUVERNANCE ET ORGANISATION

38 - Définir et coordonner les actions du ministère

L'objectif recherché consiste en un déploiement maîtrisé et accéléré de l'intelligence artificielle dans les armées, directions et services. Pour atteindre cet objectif, une gouvernance spécifique au ministère s'impose. Elle reposera sur **3 niveaux : un « noyau dur »** et deux cercles concentriques.

➢ Créer une Cellule de Coordination de l'Intelligence Artificielle de Défense (CCIAD), rattachée à l'AID et comportant une dizaine de membres, chargée d'animer les actions ministérielles en faveur de l'IA.

La compétence en IA du ministère se structurera autour d'une **Cellule de Coordination de l'Intelligence Artificielle de Défense (CCIAD)** placée au sein de l'Agence innovation défense La CCIAD a un rôle de facilitateur de l'implémentation de l'IA, de coordination des différents projets et actions et d'organisation et de pilotage des travaux transverses (veille technique et industrielle, animation de l'écosystème, travaux méthodologiques, contribution aux travaux interministériels). Cette équipe permanente et pluridisciplinaire comprend une dizaine d'experts pilotés par un directeur de projet, coordinateur ministériel. Ces personnes lui sont rattachées fonctionnellement et maintiennent un lien étroit avec les différents acteurs de leur entité d'origine où elles ont vocation à impulser la démarche et à coordonner des actions. Cette cellule pilote bénéficie par ailleurs de la collaboration des membres du premier cercle.

Premier cercle

Le premier cercle participe très activement à l'animation et à la coordination des activités liées à l'IA dans les différentes entités. Ses membres sont les interlocuteurs de la CCIAD dans les organismes du ministère, les porteurs des cas d'usage spécifiques à chaque milieu et les relais des bonnes pratiques. Ce cercle joue donc un rôle essentiel dans l'efficience du dispositif et dans la diffusion de la culture de l'IA au sein du ministère.

Il comprend :

- Les coordonnateurs IA des armées, directions et services ;

- Les responsables des actions transverses pouvant concerner l'IA (par exemple : responsables des actions sur l'éthique ou le cadre légal) ;
- Les responsables de groupes thématiques ayant un lien avec.

Second cercle

Le second cercle, plus large, vise à mettre en œuvre de manière concrète, les orientations et les impulsions données par la CCIAD et le premier cercle. Ils informent régulièrement ce dernier de leurs avancées, de leurs besoins éventuels en soutien et en orientation si nécessaire.

Il comprend les responsables de projets et d'actions qui intègrent une solution en matière d'intelligence artificielle. Il s'agit :

- Pour la DGA : d'un architecte fonction IA ou un expert IA qui intègrera l'équipe de toute opération d'armement ayant un module d'IA ou de toute étude amont en lien avec l'IA ;
- Pour* les armées, directions et services : d'officiers porteurs d'expérimentations dans les Labs, les forces ou les instances d'acculturation et de formation (écoles d'officiers...).

La DGA a par ailleurs créé un nouveau métier intitulé DIA (Data sciences et Intelligence Artificielle) dont les experts et les architectes constitueront les ressources essentielles du ministère sur l'ingénierie du « cœur de l'IA ».

Mise en œuvre de la gouvernance

Cette structure fédératrice présidée par le Coordinateur ministériel comprend les armées, directions et services, étant entendu que la partie « données » demeure traitée dans le cadre de la commission ministérielle des données. Elle organise et suit les différents travaux, examiner les nouvelles actions à lancer à différentes échéances temporelles, partager des informations sur les évolutions techniques, d'usages, de l'écosystème et les actions en cours.

En complément, le Coordinateur ministériel rend compte de l'avancement du projet d'ensemble au Comité de pilotage Innovation Défense, présidé par le DGA, qui fixera les grandes orientations.

39 - Diffuser une culture volontariste d'usage de l'IA dans le ministère

Le management de haut niveau du ministère ainsi que les différents échelons de commandement opérationnels devront être sensibilisés de manière adaptée à l'intelligence artificielle, ce qui leur permettra de mieux appréhender son utilisation et de juger les projets d'investissement significatifs en la matière.

Les personnels du ministère devront être acculturés à l'IA. Le passeport numérique mis en place par la DGNUM pourra comporter à l'avenir des connaissances élémentaires sur le sujet. Cette large acculturation contribuera à la fois au travail sur les usages et à la réussite des déploiements lorsque ceux-ci seront effectifs.

À cette fin, la CCIAD sera chargée de la coordination des actions de formation continue et de formation spécifique de l'ensemble des personnels du ministère. Les membres des deux cercles de gouvernance de l'IA répercuteront les orientations et les bonnes pratiques au sein de leurs organismes. Ainsi l'ensemble du ministère sera peu à peu irrigué par la culture de l'IA.

La mise en place d'une communauté d'intérêt des personnels souhaitant utiliser l'IA a vocation à être la plus large possible. Des cercles sectoriels sont en cours de mise en place comme celui du « *big data analytic*s pour la maintenance » (organismes de soutien, états-majors et DGA/DO/SMCO).

40 - Gagner la bataille des compétences

Le recrutement des talents en intelligence artificielle fait l'objet d'une forte concurrence à l'échelle mondiale. Les grands industriels du numérique investissent en France dans des centres de R&D en IA, notamment en Île-de-France.

41 - Quels savoir-faire internes détenir ?

Des compétences en intelligence artificielle sont indispensables pour connaître l'état de l'art du domaine et pour orienter les choix du ministère sur les cas d'usage l'intéressant. Ces compétences doivent être détenues en propre lorsque certaines **tâche**s sont jugées particulièrement sensibles.

Pour les armées, directions et services, les travaux ont permis d'identifier les métiers nécessaires pour mener des projets intégrant une composante IA. À partir de ces métiers et de leurs activités, une première estimation des besoins a été réalisée et devra être consolidée et approfondie. Au global, elle fait apparaitre un besoin pour les métiers spécifiques IA d'environ 80 spécialistes en 2020 dont le nombre sera porté à environ 200 en 2023, la plupart (130) étant employés à la DGA.

42 - Comment les acquérir/préserver ?

La rareté des compétences nécessite de cibler le recrutement et de fidéliser les talents en entretenant leur motivation.

Le secteur privé étant actuellement déficitaire dans le domaine de l'IA, il offre rapidement des postes de responsabilité à des ingénieurs encore peu expérimentés, avec des salaires significatifs notamment en région parisienne.

La diversité des applications de l'IA dans le domaine de la défense et la manipulation de données très spécifiques peuvent constituer des sources de motivation pour de jeunes ingénieurs. Ces derniers apprécieront la possibilité d'expérimentation et de test que le ministère pourra leur offrir. Ils apprécieront également de pouvoir poursuivre le développement de leur expertise en étant impliqués dans des projets à forte composante technique et/ou scientifique conduits notamment dans le cadre de partenariats structurants, avec des organismes de recherche. Ils pourront également apprécier d'être associés à des enjeux opérationnels majeurs, et être au contact direct des acteurs du monde opérationnel, ce que peut difficilement offrir le monde civil.

Enfin, le recours à des recrutements d'officiers commissionnés parmi des personnels d'active ou de réserve est aussi à envisager dans certains cas pour compléter le vivier d'experts.

Les métiers de l'IA vont connaître un essor sans précédent, il conviendra d'adapter nos filières et de mener une approche métier en deux niveaux complémentaires : un groupe d'experts à la pointe de la technologie et des référents avec double compétence dans chacun des métiers impactés.

Le domaine de l'IA est riche en techniques et en applications. La veille est indispensable et doit porter sur les aspects technologiques, les projets, les produits et les innovations d'usages.

43 - Stratégie d'innovation, de recherche et de développement

L'intelligence artificielle, sujet fortement dual, ne peut progresser au sein du ministère que grâce à une interaction étroite avec le milieu civil, tant industriel qu'académique. Le pilotage de cette interaction doit permettre à la fois de susciter l'innovation et la recherche sur des sujets spécifiques et de capter les développements utilisables dans les systèmes des armées, directions et services.

44 - Des partenariats académiques privilégiés, en cohérence avec la stratégie nationale

La stratégie du Ministère des armées en matière de R&D s'inscrit en synergie avec le volet recherche de la stratégie gouvernementale, opéré par l'Agence Nationale de la Recherche (ANR).

Le ministère s'appuiera par ailleurs sur :

- des organismes de recherche fondamentale, comme l'INRIA ou le CNRS ;
- des écoles d'ingénieurs ;
- des acteurs sectoriels, capables de traiter les problématiquesspécifiquesdechaquesystème.

Cette démarche permettra par ailleurs de promouvoir l'intérêt pour les thématiques de défense parmi les futurs spécialistes de l'intelligence artificielle formés dans ces établissements.

➢ Mettre en place des partenariats structurants avec les principaux organismes de recherche académique ayant des compétences significatives en IA.

45 - Orienter la recherche vers les systèmes critiques

Les utilisations de l'IA pour le ministère des Armées présentent des caractéristiques et des exigences qui ne sont pas forcément celles des utilisations développées à ce stade pour le secteur commercial.

Ces différences font notamment apparaître de réels enjeux techniques qui sont encore loin d'être résolus. En effet, et en dépit des progrès indéniables accomplis ces dernières années, il reste encore beaucoup à faire pour aller au-delà d'applications permettant d'effectuer de manière automatisée des tâches élémentaires ou très spécialisées (jeu de go, robot aspirateur).

Par de nombreux aspects, ces défis sont similaires à ceux que devront relever tous les systèmes critiques intégrant de l'IA, qu'il s'agisse du véhicule autonome ou des systèmes de distribution d'énergie. Aussi le ministère des Armées s'emploiera-t-il à orienter et soutenir les recherches académiques et industrielles dans le domaine de l'IA pour les systèmes critiques.

➢ Orienter prioritairement les recherches académiques et les études industrielles vers les défis techniques à relever pour l'intégration de l'IA dans les systèmes critiques.

Exemple : navigation de drones en zone urbaine

En 2018, le ministère a financé au CEA/LIST 4 projets permettant de répondre en mode « quick win » à des cas d'usage proposés par le ministère. Le CEA/LIST constitue un centre d'excellence en matière d'IA, avec plus de 200 chercheurs se consacrant à ce domaine. Le modèle CEA de valorisation de la recherche sous forme de spin-off s'applique pleinement dans le domaine de l'IA, avec la création de plus de 20 start-ups issues de ses laboratoires de recherche sur les 5 dernières années (Diota, Tridimeo, Sybot, etc.).

L'usage de drones de reconnaissance s'impose de plus en plus dans les armées du monde, en raison de leur relative discrétion, et surtout de la réduction du risque pour le soldat. La navigation et la cartographie dans les zones dégagées sont un problème relativement simple, mais dans des environnements urbains denses, une navigation sous la hauteur des bâtiments pose des problèmes non-triviaux de détection d'obstacles, et la cartographie d'un lieu présente de nombreux défis algorithmiques. Le projet va traiter la localisation et relocalisation basées sur la vision, la reconstruction 3D temps réel avec segmentation des obstacles et la reconstruction 3D fine en temps différé, la détection et le suivi d'objets mobiles d'intérêt (véhicules, piétons) et la segmentation sémantique en mode monoculaire. Ci-dessous une illustration de l'algorithme à base de deep learning pour la détection et la localisation 3D temps réel de véhicules en vision monoculaire (technologie Deep Manta) :

46 - Des investissements en forte croissance

Afin de préparer les futures applications de l'IA à horizon 10 ans, le ministère des armées investira massivement dans les études et la recherche. Durant la période de la présente Loi de Programmation Militaire 2019-2025, le ministère investira près de 430 M€ d'études amont au profit de l'intelligence artificielle. Cet effort sera concentré d'une part sur la stimulation et la captation de l'innovation duale, et d'autre part sur le financement des applications spécifiques à la défense.

Figure 5 – Répartition des efforts d'investissement sur l'IA en fonction de la dualité et de la maturité technique.

Cet investissement devra permettre de répondre aux besoins immédiats des armées (temps court) tout en s'inscrivant aussi dans la préparation de l'avenir (temps long). À cette fin, le ministère peut s'appuyer sur une palette d'outils de soutien à l'innovation développés depuis plusieurs années par la DGA (Thèses, dispositifs ASTRID et RAPID, challenges ANR-DGA[14]), en complément de son socle historique de conduite de projets de R&T et de programmes d'armement. L'AID, récemment créée, a vocation à enrichir cette palette et à en permettre une mise en œuvre plus efficace et plus agile.

Exemple : les challenges MALIN (maîtrise de la localisation indoor) et DEFALS (Détection de Falsification)

Co-organisée et financée par la DGA et l'Agence Nationale de Recherche (ANR), une compétition technique d'une durée de 3 ans, sous le nom de MALIN (Maîtrise de la localisation Indoor, visant à identifier des solutions de géolocalisation en l'absence de signal GPS dans des environnements difficiles), a été lancée en décembre 2017. Les six équipes participantes, réunissant industriels et laboratoires académiques, s'affrontent régulièrement à l'occasion d'épreuves de difficulté croissante. Il s'agit de les faire progresser en mesurant précisément leurs performances et en identifiant leurs points forts et leurs points faibles. Différentes technologies « capteurs » sont mises en œuvre dans les dispositifs testés en situation (vision stéréo, lidar, centrales inertielles, magnétomètres, etc...). L'efficacité et la robustesse du système reposent alors sur le traitement et l'analyse des signaux collectés : les techniques de fusion de données et d'intelligence artificielle sont alors déterminantes ; en appui des technologies, des méthodes d'IA peuvent, par exemple d'analyser la démarche d'un fantassin au cours de son déplacement et d'optimiser ainsi la restitution de sa trajectoire.

14 Le dispositif « challenges » consiste à organiser une compétition entre plusieurs équipes de recherche vis-à-vis d'une finalité applicative donnée, et destinée à faire progresser l'état de l'art scientifique dans le domaine.

Illustrations du challenge MALIN

Le challenge DEFALS, actuellement en cours, obéit au même principe d'émulation. Il vise à :

- *Initier et faire progresser la recherche en analyse d'images à des fins de vérification d'intégrité (détection aveugle de modification dans des images réelles) ;*
- *Mobiliser les communautés du traitement de l'information, et susciter des rapprochements entre différentes disciplines. Les corpus sont composés de prises de vue de scènes naturelles d'intérieur et d'extérieur, de scènes urbaines et de paysages, etc...*

Le développement d'outils fiables et automatisés permettrait de lever le doute sur une information qui peut notamment porter un préjudice à personne physique, une société ou un organisme (ex. : retouche d'images de presse, canular industriel) ou créer un faux événement (ex. : enrichissement de données à des fins de propagande).

47 - Évaluer, « benchmarker », pour un investissement avisé

Afin d'orienter son investissement en R&D de manière avisée, le ministère évaluera de manière systématique les résultats des études et des recherches financées. Cette évaluation devra être qualitative mais également **quantitative** en utilisant des métriques spécifiques aux systèmes contenant de l'IA. Pour concevoir, développer et mettre en œuvre ces métriques ainsi que les jeux de tests associés, le ministère des armées s'appuiera sur la compétence du Laboratoire National de Métrologie et d'Essai. Le ministère promouvra par ailleurs ce modèle en interministériel.

48 - Passer à l'échelle industrielle

Afin de faciliter le passage à l'échelle industrielle des systèmes contenant de l'IA, le ministère des Armées mènera en étroite cohérence, sous le pilotage de la CCIAD, sa stratégie d'innovation et sa stratégie d'acquisition.

➢ Mettre en place et piloter des mécanismes entre les contrats de recherche et l'acquisition de solutions pour faciliter le passage à l'échelle industrielle.

Par ailleurs, la mise en œuvre d'une stratégie de R&D dans le domaine de la défense nécessite de faire monter en maturité le sujet chez les MOI Défense. Il conviendra d'accompagner les grands industriels systémiers de défense pour qu'ils réfléchissent à l'utilisation de l'intelligence artificielle dans leurs systèmes, qu'ils soient capables d'intégrer rapidement des modules à base d'intelligence artificielle (y compris développés par des tiers) et qu'ils développent des compétences dans les cas spécifiquement militaires (ex : traitements pour capteurs militaires : radars, sonars, guerre électronique...).

49 - Coopération internationale et stratégie à l'export

L'IA est un domaine privilégié de coopération internationale de par sa nature duale et la possibilité d'accéder de manière ouverte à un grand nombre d'algorithmes et de données. Les coopérations en matière d'usage militaire peuvent prendre plusieurs formes selon l'ambition politique recherchée, le niveau de maturité des briques technologiques, la sensibilité du projet aux critères éthiques ou selon la proportion de l'IA dans l'intégralité du programme de coopération (simple incrément ou brique structurante).

Pour choisir avec discernement les coopérations envisageables, il convient dès lors de bien identifier le but recherché – notamment, identifier le cas d'usage qui sera forcément limité, puis de cerner les contraintes qui se posent dans l'immédiat ou à moyen terme.

50 - Des coopérations aux objectifs stratégiques variés

La revue stratégique de défense et sécurité de 2017 a rappelé que « ... la maîtrise de

l'intelligence artificielle représentera un enjeu de souveraineté… [15]», ce qui n'exclut pas la possibilité de développer des coopérations fortes, en particulier au niveau européen. Cela peut se faire selon différents cas de figure en fonction des objectifs recherchés :

51 - Objectifs politiques : coopération structurelle ou d'opportunité

Ainsi, nos coopérations IA peuvent s'inscrire dans un cadre européen seul cadre pertinent pour réellement développer de puissantes synergies, comme le propose la stratégie IA de l'UE. L'Allemagne et le Royaume-Uni sont deux partenaires incontournables dans cette optique.

Hors continent européen, d'autres États importants souhaitent s'affranchir du duopole IA exercé par la Chine et les États-Unis. Il peut à cet égard y avoir convergence d'intérêt, surtout si d'autres coopérations croisées se mettent en place.

52 - Objectifs industriels et technologiques : complémentarité ou consolidation

La coopération peut également viser un avantage industriel ou technologique ; on peut distinguer deux cas de figure :

- **Complémentarité** : la coopération peut renforcer notre position nationale en palliant une carence partielle ou totale. Cette complémentarité peut être recherchée à une échelle structurelle (politique industrielle ou recherche) ou de manière ciblée (projets sur un segment précis de l'IA). Elle pourra prendre la forme d'alliances industrielles ou de partenariats entre centres de recherche.
- **Consolidation** d'un avantage comparatif : la coopération cherche à capitaliser sur un atout commun à plusieurs pays pour le démultiplier ou pour atteindre une masse critique (mise en commun des moyens de recherche, de volumes de données suffisants, création d'une grande entité intégratrice en matière d'IA, …). Ce type de coopération serait à privilégier dans le cadre européen.

53 - Objectifs de performance militaire : critère essentiel pour le ministère des Armées

Les partenariats ne sont pas à envisager uniquement sous l'angle capacitaire et industriel. En effet, l'interopérabilité des forces est un facteur essentiel de succès des engagements opérationnels en coalition. C'est un impératif pour la France, nation-cadre et assumant un rôle de leader ou de contributeur de premier plan. Les coopérations militaires en matière d'IA doivent contribuer à atteindre cet objectif majeur. Les coopérations militaires en matière d'IA pourront viser à concevoir, puis mutualiser des équipements militaires valorisés par l'IA, mais aussi englober d'autres champs comme le soutien, la logistique, la simulation, la formation, l'organisation ou encore le partage du renseignement. Dans tous les cas, ces liens de coopération pourront s'inscrire dans différents types de format, qu'il s'agisse de cadres bilatéraux ***ad hoc*** ou de cadres déjà existants (CSP)[16].

Quelle que soit la nature du partenariat envisagé, la question de la classification des données se posera et obligera à penser en amont les modalités de leur partage, selon la sensibilité du domaine de coopération et la profondeur du lien politique entretenu.

> ➢ Au niveau européen, rendre visible notre position Défense et poursuivre les discussions avec nos partenaires, en coopération avec le SGAE et le MEAE.

Les 7 axes d'effort prioritaires se prêtent à des coopérations à des degrés divers. Les sujets identifiés à ce stade qui ne posent pas de problème de maintien ou de développement de compétences ou de partage de données classifiées sont les suivants :

- aide à la décision et à la planification : systèmes de conduite des opérations au niveau stratégique et de planification dont notamment la logistique (avec la maintenance prédictive) ;
- combat collaboratif : les interfaces homme-machine, l'entraînement augmenté ;
- logistique et maintien en condition opérationnelle : les applications de performances en mission et maintenance assistée, notamment pour des coopérations avec les pays ayant les mêmes systèmes que les nôtres ;
- renseignement : les outils de fouille et de synthèse de données ;
- robotique et autonomie : les modules de comportements évolués des robots (hors robots / drones engagé dans les domaines de lutte, ainsi que ceux emportant des capteurs spécialisés hautement sensibles) ;

Pour les applications transverses et de soutien, les

15 Revue stratégique, § 256, page 74.

16 Coopération structurée permanente.

coopérations sont plus facilement envisageables, notamment dans le domaine de la **médecine du futur.**

54 - Différents cercles de coopération potentiels

La prise en compte des critères précédents permet d'envisager trois cercles de coopération possibles. Ces trois cercles peuvent évoluer de manière dynamique, compte tenu d'un contexte général loin d'être figé.

55 - Premier cercle : les partenaires structurants

Il est constitué de nos partenaires européens majeurs avec lesquels la coopération en matière d'IA est déjà partie intégrante d'une relation bilatérale mature et développée, structurée par de grands programmes. La coopération répond donc ici à un ensemble d'objectifs pluridimensionnels : politiques (autonomie stratégique confortée, approfondissement des liens), industriels (atteinte d'une taille critique dans différents segments ou valorisation d'atouts différents) et militaires (coopération capacitaire, doctrinale, gouvernance).

Outre ces nations partenaires de premier plan, l'OTAN et en particulier ACT offrent un cadre privilégié de coopération.

56 - Second cercle : les partenaires dimensionnants

Le second cercle réunit les **États-Unis**, l'**Australie** et l'**Inde**, certes non-européens mais déjà partenaires. Ils adoptent des approches similaires aux nôtres en matière d'IA et notre coopération avec eux a vocation à s'étendre à l'IA de défense. Première puissance IA, les États-Unis ont exprimé la volonté de coopérer avec leurs alliés-clés, dont la France. L'Australie et l'Inde se sont engagés sur le long terme (sous-marins Barracuda, acquisition de Rafale) ; tous ces projets incorporeront des briques technologiques IA significatives, tant en conception que lors des futurs ***retrofits***.

57 - Troisième cercle : les partenaires d'opportunité

Le troisième cercle regroupe les pays avec lesquels des opportunités de coopérations ciblées sont susceptibles de se manifester : partenaires européens ou non-européens avec de réelles capacités ou appétences en IA (**Canada, Japon, Singapour, Corée**). Ces coopérations pourront couvrir l'ensemble des domaines : capacitaire, doctrine, échange de renseignement, formation, débat éthique. Ces coopérations d'opportunité peuvent constituer l'amorce de partenariats IA plus intégrés.

Ce tableau en trois cercles n'indique pas pour autant une vision uniquement bilatérale de nos coopérations IA. Au contraire, des partenariats croisés entre plusieurs acteurs ont vocation à fertiliser ces coopérations et peuvent s'entendre entre partenaires européens ou avec nos partenaires privilégiés de la zone indopacifique.

CONCLUSION

Ainsi, au terme de ces travaux, les principales orientations pour l'action du ministère des Armées en matière d'Intelligence Artificielle sont les suivantes :

la création d'un comité ministériel destiné à se prononcer, en particulier mais de manière non exclusive, sur les questions éthiques que pourraient soulever les développements futurs de l'IA appliquée au domaine militaire ;

le développement et le maintien d'un vivier d'experts au sein du ministère ;

la mise en place d'une politique ministérielle de la donnée qui doit garantir une exploitation optimale des données tout en respectant les exigences de sécurité et de conformité ;

une feuille de route capacitaire solide pour une intégration responsable et maîtrisée de l'IA au sein de nos forces, comme dans le fonctionnement plus général du ministère, dans le respect des valeurs que notre pays défend partout dans le monde ;

la mise en place d'une gouvernance de l'action ministérielle en IA, avec la création d'une Cellule de Coordination de l'IA de Défense (CCIAD) au sein de l'Agence ID ;

l'établissement de partenariats stratégiques avec les acteurs de l'innovation et de la recherche en pointe sur le sujet ;

la mise en place de mécanismes entre les contrats de recherche et l'acquisition de solutions pour faciliter le passage à l'échelle industrielle ;

le développement de coopérations internationales, en particulier au niveau européen, afin de porter nos positions stratégiques et de peser dans l'établissement des normes techniques ou des régulations sur l'export des technologies à base d'IA.

Le cap ainsi fixé permettra au ministère des Armées de tirer profit de la révolution technologique engagée, sans renier les valeurs et fondements de son action, en opérations comme dans son fonc-

tionnement courant.

ANNEXE

L'INTELLIGENCE ARTIFICIELLE, UN DOMAINE AUX VASTES TECHNIQUES

Le domaine de l'***intelligence artificielle*** possède une délimitation variable en fonction des interlocuteurs, la frontière évoluant également au cours du temps (les langages à objets sont nés de travaux sur l'IA pour représenter des données symboliques et sont considérés comme des outils de l'informatique « classique » depuis les années 80).

Nous adoptons ci-après une définition assez large, couvrant 4 principaux domaines de recherche.

- **L'apprentissage automatique :** famille d'algorithmes qui prend en entrée un corpus de données (ou un simulateur de données) annotées en fonction de la tâche à effectuer et qui produit en sortie un modèle capable de reproduire le comportement attendu sur le corpus initial et de généraliser ce comportement de manière pertinente sur de nouvelles données. Le volume de données, le type et le volume d'annotation et les cas applicatifs varient grandement en fonction de chaque classe d'algorithme. L'apprentissage par renforcement s'applique par exemple en priorité aux problèmes impliquant une boucle observation-action comme la robotique autonome ou aux jeux aux règles bien définies. Les réseaux de neurones sont quant à eux à la pointe de la recherche pour le traitement de données de très grandes dimensions, en particulier les données non structurées (texte, son, image...), mais d'autres familles notamment issues des statistiques peuvent se révéler aussi performantes et plus simples d'usage dans le cas de données de faible dimension ou pour les données plus structurées.

- **La gestion des connaissances et le raisonnement :** famille d'algorithmes servant à structurer la représentation des connaissances, la recherche et l'inférence d'informations à partir de règles explicites. Ce sont des approches permettant de prendre en compte très efficacement des connaissances a priori fournies par des experts métiers. Mais ce sont aussi les approches ayant contribué à l'origine du premier hiver de l'IA au travers d'annonces beaucoup trop optimistes sur leurs capacités : dès que l'on s'intéresse à des problèmes trop vastes, il devient rapidement très compliqué de modéliser suffisamment correctement le domaine pour pouvoir y appliquer avec succès ces méthodes.

- **La recherche opérationnelle :** famille d'algorithmes qui consiste à rechercher une solution à un problème d'optimisation, qui peut contenir un ou plusieurs objectifs à optimiser, et une ou plusieurs contraintes que la solution doit respecter. Certaines approches fournissant de plusieurs solutions de compromis à des problèmes multi-objectifs, permettant de choisir a posteriori celle convenant le mieux en fonction de l'importance que l'on attache à chacun des objectifs. La recherche de solutions exactes ou optimales requiert très souvent une puissance de calcul exponentielle, en fonction du nombre d'objectifs et de contraintes à satisfaire. Aussi, cette branche de l'IA s'intéresse notamment à identifier des heuristiques permettant de limiter l'espace de recherche et de trouver des solutions relativement proches de l'optimum en un temps de calcul raisonnable.

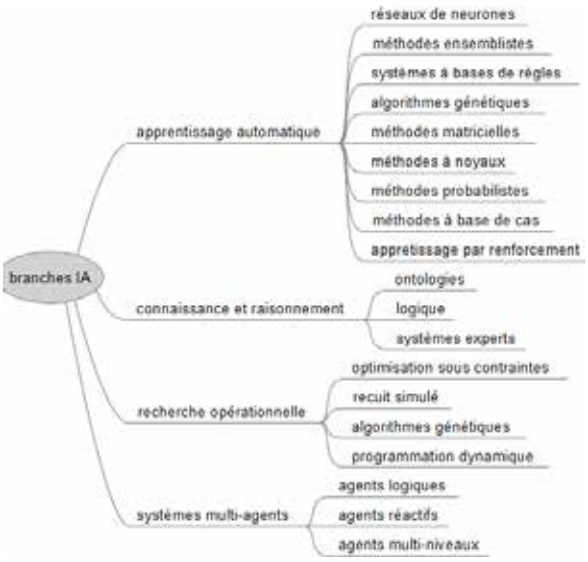


Figure 6 - Visualisation des grandes branches de l'intelligence artificielle

- **Les systèmes multi-agents :** famille d'algorithmes qui servent à gérer de manière décentralisée un système dans lequel de nombreux agents interviennent. Cette branche permet de répondre à des problématiques diverses, comme la mise en œuvre d'essaim d'agents de faible capacité individuelle mais permettant de faire émerger collectivement un comportement / fonctionnalité évolué (sur le modèle d'une colonie de fourmis), mais également la coordination de systèmes autonomes plus complexes (l'humain pouvant faire par-

tie de ces systèmes comme ensemble de sous-systèmes collaborant), ou encore la simulation de systèmes complexes.

Si les techniques élémentaires suffisent pour réaliser des tâches ciblées (ex : reconnaissance de visages), plus on cherche à réaliser des tâches complexes ou des tâches variées et plus il est nécessaire de combiner des algorithmes entre eux et d'utiliser des jeux de données variées.

Dans la version américaine de « questions pour un champion », IBM a dû mettre en œuvre des fonctions pour transcrire la voix en texte, analyser le texte pour en déduire les informations recherchées, fouiller plusieurs bases de données, choisir la meilleure réponse estimée et la restituer en langage naturel.

Pour le véhicule sans chauffeur sur tout type de route (capacité de niveau 5), il faudra être capable de planifier le chemin et de le replanifier (travaux, embouteillages…), de positionner le véhicule, de détecter et analyser le comportement des autres mobiles (véhicules, cyclistes, piétons, animaux…) et de prédire si ce comportement est susceptible d'entrer en conflit avec son propre déplacement, de respecter la signalisation et le code de la route. Les experts du domaine estiment que l'atteinte du niveau 5 pourrait encore nécessiter de l'ordre d'une dizaine d'années.

Le cas d'un robot terrestre « autonome » pour des applications militaires est plus complexe : l'accès à un système de positionnement global type GPS n'est pas garanti (environnement non coopératif), les déplacements doivent être possibles hors route (environnement non structuré), les comportements externes à surveiller ne sont pas uniquement à proximité (les tirs ennemis peuvent provenir de mobiles éloignés et également des airs), les tâches à réaliser peuvent être plus variées que se déplacer d'un point à un autre…

Il faut noter que l'ensemble de ces techniques ne permet pas actuellement de reproduire des capacités d'intelligence semblables à celles de l'esprit humain pour aborder n'importe quelle situation et y réagir en conséquence. Un tel challenge est considéré par beaucoup d'experts comme une perspective lointaine voire peu crédible comme le mentionne le rapport de la mission Villani.

ÉLÉMENTS DE L'ÉTAT DE L'ART EN INTELLIGENCE ARTIFICIELLE

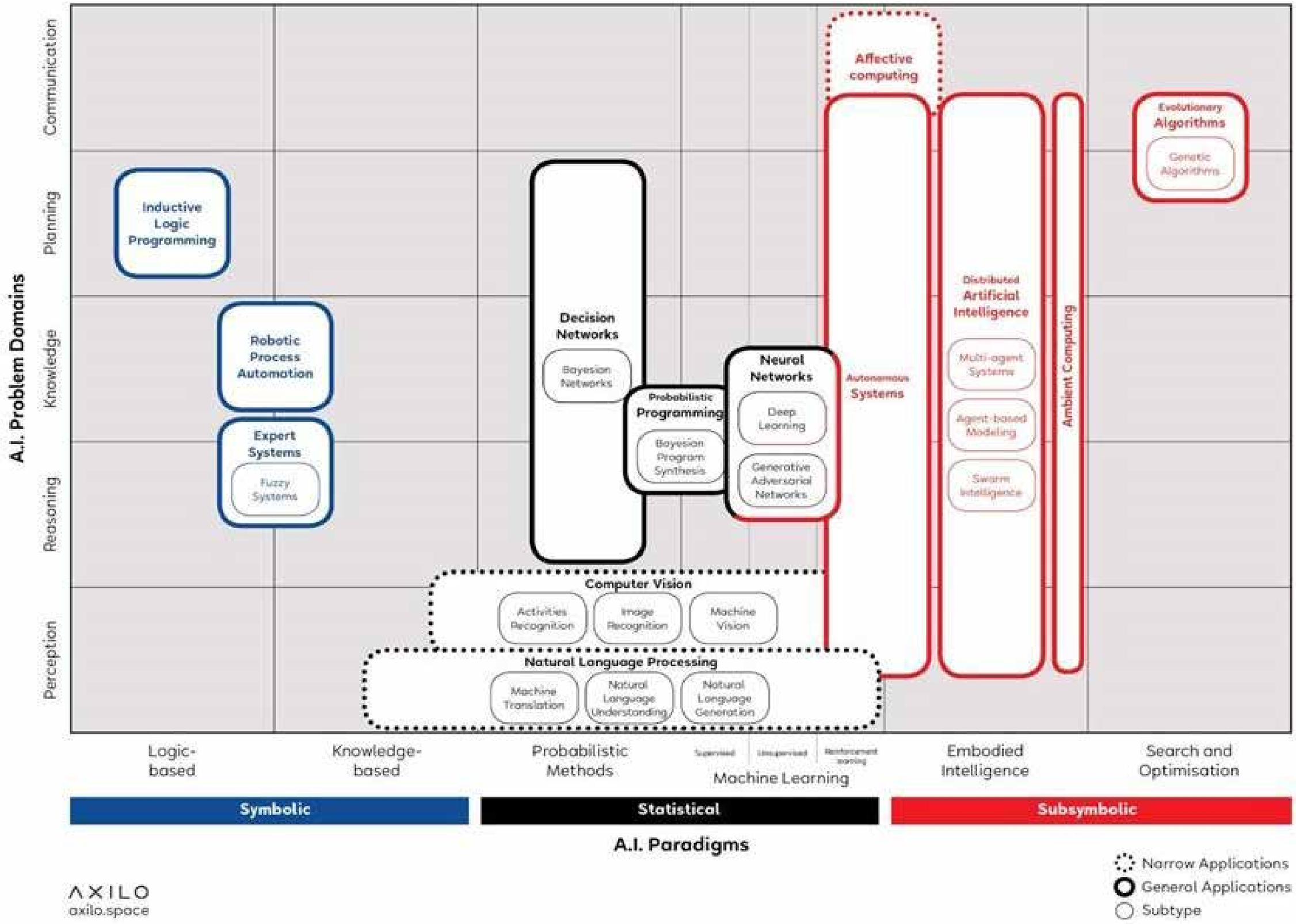
Le tableau ci-après donne un éclairage de l'état de l'art accessible actuellement pour de grandes branches applicatives de l'intelligence artificielle et mentionne les limitations actuelles avec en **gras*** celles qui sont d'intérêt particulier pour le secteur de la défense et parfois peu explorées par le secteur civil.

En plus des limitations citées dans le tableau qui doivent faire l'objet d'efforts de recherche, il est possible de mentionner quelques grands challenges actuels particulièrement importants dans le domaine de la défense : la robustesse (fiabilité et qualification des méthodes à réseaux de neurones, confidentialité des modules d'IA), l'embarquabilité (réduction des besoins en calcul, coordination distribuée), l'adaptabilité (détection d'anomalies de fonctionnement), la simplification des processus d'apprentissage (utilisation de données simulées, apprentissage frugal, apprentissage non (ou moins) supervisé), les interfaces homme/IA (explicabilité des sorties de modules d'IA, contrôle d'essaims d'agents autonomes, nouvelles méthodes d'interaction). Il faudra également examiner les voies techniques prometteuses pour espérer de nouvelles ruptures de performances (ex : approches mixtes symboliques / connexionnistes) et suivre les développements des ordinateurs quantiques qui pourraient balayer certains problèmes calculatoires de l'IA.

À PROPOS DES CALCULATEURS POUR L'INTELLIGENCE ARTIFICIELLE

Les besoins en puissance de calcul dépendent du type de technique algorithmique et des applications :

- Techniques d'IA avec apprentissage à partir de données brutes :
    - Besoins pour l'apprentissage proprement dit : grosses capacités de calcul avec accès centralisé aux données ;
    - Besoins pour l'utilisation (« inférence ») : les besoins en calculs sont bien moins importants, mais on peut faire face à des contraintes du type temps réel / applications embarquées.
- Techniques d'IA sans apprentissage (comprend notamment la recherche opérationnelle) : les besoins de capacités de calcul sont plus ou moins importants selon les applications.



AXILO
axilo.space

Maturité par grande famille applicative

	Performances actuelles	Limitations
Traitement de la parole / langage	- Transcription, Traduction automatique de langues courantes - Traduction écrite automatisable > 80%	- **Environnement bruité*** - **Langues moins répandues / rares*** - Compréhension du texte (sémantique)
Traitement des images, vidéos, capteurs	- Interprétation d'images médicales (> Homme) - Reconnaissance d'objets dans des images (~ Homme) - Détection et suivi automatique de mobiles	- Nombre d'objets à reconnaître, **objets de faible résolution**, - **Autres capteurs que caméras dans le visible*** - Taille des bases d'apprentissage
Optimisation	- Planification de trajectoire en 2D - Affectation de ressources sous contraintes	- **Planification 3D, re-planification en ligne (+ embarqué)*** - Temps de calcul, solution non optimale
Fouille, Extraction d'information	- Identification automatique de données similaires, d'éléments atypiques (sur données majoritairement structurées) - Identification des sources d'information les plus pertinentes	- **Données hétérogènes, maj. non structurées, distribuées*** - Découpage en sujets / questions élémentaires - Modélisation des connaissances sur larges domaines - Compréhension sémantique, détection de « fake news »
Raisonnement	- Chatbot automatisant une liste de FAQ - Diagnostic avec une cause principale - Robot pour tâche simple (ex: robot tondeuse) en environnement peu évolutif et semi-structuré (ex : routes + GPS) - Aides à la décision sur problèmes facilement modélisables - Jeux avec règles et nombre de positions finies (échec, go)	- Chatbot généraliste - Diagnotic avec causes multiples - **Robot multiples tâches, environnements évolutif et non structuré***, Planification et contrôle de groupes de robots - **Aides à la décision sur problème difficilement modélisable (ex : situation militaire)*** - Jeux complexes

** caractéristiques prégnantes pour les applications militaires*

La plupart des méthodes d'IA peuvent se satisfaire de calculateurs généralistes (CPU conventionnels). Pour les phases d'apprentissage, des ordinateurs de bureau ou des serveurs de calcul suffisent si la base d'apprentissage reste de taille limitée. Néanmoins, l'apprentissage d'un réseau de neurones est très gourmand en ressources de calcul et en mémoire. Les calculateurs les plus efficaces pour cette tâche sont les GPU, dans l'idéal des GPU dédiés au calcul scientifique sous forme de serveurs qui disposent notamment de plus de mémoire dédiée que les GPU classiques.

La phase d'inférence peut utiliser des machines semblables (non embarquées) afin de traiter de gros volumes de données. L'inférence des réseaux de neurones se fait également très bien sur GPU. Si on a une application embarquée avec des réseaux de neurones, il y a plusieurs solutions envisageables en termes de cible matérielle embarquée en tenant compte des outils de portage logiciel :

- Les CPU (***Central Processing Unit***) embarqués, conviennent pour les petits réseaux de neurones, ou ceux qui n'ont pas de contraintes temps réel. Mis à part le passage en virgule fixe, le portage est simple.
- Les GPUs embarqués (ex : NVidia Tegra TX) offrent de bonnes performances pour une faible consommation. Le travail de portage reste limité.
- Les DSP (Digital Signal Processor), offrent de meilleures capacités qu'un CPU embarqué, de faibles besoins énergétiques mais un travail de portage moyen (ex : Texas Instrument C6x).
- Les processeurs massivement parallèles (MPPA de Kalray par exemple) offrent de bonnes capacités de calcul, mais requièrent un portage complexe.

Une implémentation matérielle dédiée (FPGA ou ASIC) est toujours possible pour les applications fortement contraintes, mais elle nécessite un coût de portage élevé car les bibliothèques d'exploitation sont peu fournies. Concernant les FPGA, le développement d'une gamme durcie et temps réel pour les applications spatiales est en cours pour s'affranchir des États-Unis (projet MARS / NanoXplore, STM).

Le succès d'un calculateur pour l'IA dépend en très grande partie de l'écosystème logiciel qui l'entoure, en particulier les bibliothèques de primitives bas et moyen niveaux. Ceci explique l'hégémonie de NVidia dans les GPU pour réseaux de neurones via la mise à disposition d'un outil de programmation de ses cartes (CUDA) avec une surcouche pour réseaux de neurones (CuDNN). Ces bibliothèques ont permis le développement des grands ***frameworks*** (Tensorflow (Google) ou Pytorch (Facebook)). Sur le sujet des bibliothèques dédiées, il faut noter le projet du CEA (N2D2) visant à faciliter le portage des réseaux de neurones sur calculateurs embarqués et le RAPID en cours avec Kalray et MBDA (projet ACADEMIS) qui développe une telle bibliothèque pour les composants MPPA de Kalray.

Si la bataille des marchés génériques de type CPU et GPU semble délicate pour l'Europe, il est encore possible d'élaborer des solutions européennes de puces adaptées à l'IA embarquée.

GLOSSAIRE

Acronyme	Définition	Contexte
3IA	Institut interdisciplinaire d'intelligence artificielle	FR
ACT	Allied Command Transformation	
ADS	Armées, directions et services	MINARM
AFNOR	Association française de normalisation	FR
AI	Artificial Intelligence	
AID	Agence d'innovation de la défense	MINARM
ANSSI	Agence nationale de la sécurité des systèmes d'information	FR
API	Application Programming Interface	
ARTEMIS	Architecture de traitement et d'exploitation massive de l'information multi-sources	DGA
ASIC	Application-Specific Integrated Circuit	
ASTRID	Accompagnement spécifique des travaux de recherche et d'innovation défense	DGA
BATX	Baidu, Alibaba, Tencent et Xiaomi	Chine
BF	Basse fréquence	TECH
BITD	Base industrielle technologique de défense	DGA
C2	Command and Control	MILI
C4ISR	Command, Control, Computers, Communications, Intelligence, Surveillance, Reconnaissance	MILI
CALID	Centre d'analyse de lutte informatique défensive	EMA
CCAC	Convention sur certaines armes classiques	ONU
CCIAD	Cellule de coordination de l'intelligence artificielle de défense	MINARM
CEA	Commissariat à l'énergie atomique	FR
CEMA	Chef d'état-major des armées	EMA
CEN	European Committee for Standardization	UE
CICDE	Centre interarmées de concepts, de doctrines et d'expérimentations	EMA
CIFRE	Convention industrielle de formation par la recherche	FR
CNRS	Centre national de la recherche scientifique	FR
CPU	Central Processing Unit	
CSO	Collaborative Support Office	
CSP	Coopération structurée permanente	UE
CUDA	Compute Unified Device Architecture	
CuDNN	CUDA Deep Neural Network	
DGA	Direction générale pour l'armement	DGA
DGNUM	Direction générale du numérique et des systèmes d'information et de communication	MINARM
DGRIS	Direction générale des relations internationales et de la stratégie	MINARM
DIA	Data sciences et intelligence artificielle	DGA
DIH	Droit international humanitaire	Intl
DIRISI	Direction interarmées des réseaux d'infrastructure et des systèmes d'information	EMA
DORESE	Doctrine, organisation, ressources humaines, équipements, soutien, entraînement	MINARM
DRI	Détection, reconnaissance, identification	MILI

Acronyme	Définition	Contexte
DSP	Digital Signal Processor	
EMA	État-major des armées	EMA
ETI	Entreprise de taille intermédiaire	FR
FIA	Foreign Intelligence Surveillance Act	US
FPGA	Field Programmable Gate Array	
FREMM	Fregate multi-missions	
FTI	Frégate de taille intermédiaire	MER
GAFA	Google, Apple, Facebook et Amazon	US
GE	Guerre électronique	MILI
GGE	Groupe d'experts gouvernementaux	ONU
GIEC	Groupe d'experts intergouvernemental sur l'évolution du climat	ONU
GPS	Global positioning system	
GPU	Graphics Processing Unit	
GT	Groupe de travail	FR
GTB	Gestion technique de bâtiment	FR
GTIA	Groupement tactique interarmes	TERRE
HF	Haute fréquence	TECH
HLEG	High-level expert group	UE
I2R	Ingénierie de l'informatique et robotique	DGA
IA	Intelligence Artificielle	TECH
IEC	International Electrotechnical Commission	Intl
IHM	Interface homme-machine	TECH
INRIA	Institut national de recherche en informatique et automatique	FR
IOT	Internet Of Things	
IR	Infra-rouge	
ISO	International Standard Organization	Intl
ITAR	International Traffic in Arms Regulations	US
JAIC	Joint Artificial Intelligence Center	US
LIST	Laboratoire d'intégration de systèmes et des technologies	FR
LPM	Loi de programmation militaire	MINARM
MALE	Medium Altitude Long Endurance	AIR
MGCS	Main Ground Combat System	
MI	Maîtrise de l'information	DGA
MMT	Man-Machine Teaming	AIR
MOD	Ministry of Defence	UK
MRTT	Multi-Role Tanker Transport	AIR
MUST	Méthodologie d'exploitation des données d'Usages des véhicules et d'identification de nouveaux Services pour les usagers et les Territoires	DGA
NAN	Non-Aligned Movement (mouvement des non-alignés)	Intl
OIV	Opérateur d'Importance Vitale	FR
ONERA	Office national d'études et de recherches aérospatiales	FR
OTAN	Organisation du traité de l'Atlantique Nord	OTAN
PIA	Programme d'investissements d'avenir	FR
PME	Petite ou Moyenne Entreprise	FR

Acronyme	Définition	Contexte
POCEAD	Plateforme d'ouverture, de centralisation, d'exposition et d'analyse des données	DGA
RAPID	Régime d'appui à l'innovation duale	DGA
RENS	Renseignement	MILI
RETEX	Retour d'expérience	MILI
RF	Radio Frequency	
RGPD	Règlement général sur la protection des données	Intl
RH	Ressources humaines	FR
ROEM	Renseignement d'origine électromagnétique	MILI
ROIM	Renseignement d'origine image	MILI
SALA	Système d'armes létales autonome	MILI
SAR	Specific Absorption Rate	TECH
SCOR-PION	Synergie du contact renforcée par la polyvalence et l'info valorisation	DGA
SGA	Secrétariat général pour l'administration	MINARM
SMCO	Service du maintien en condition opérationnelle	DGA
TRL	Technical Readiness Level	
UE	Union Européenne	UE

Contexte de l'acronyme : MINARM, DGA, EMA, AIR, TERRE, MER. FR = France, UE = Europe, OTAN, ONU, Intl = International, Chine, US, UK. TECH = Technique. MILI = Militaire.