INTELLIGENCE ARTIFICIELLE

pour les opérations terrestres

GIGAT

INTELLIGENCE ARTIFICIELLE

POUR LES OPERATIONS TERRESTRES

Contributeurs
Julien BZOWSKI (Safran.Ai)
Maud FORESTI (Arquus)
Christophe GUETTIER (Safran)
Arnault IOUALALEN (Numalis)
Eric LEBIGOT (Bertin Technologies)
Guillaume QUIN (MBDA)
Bruno RICAUD (KNDS FR)

Présidents
Juliette MATTIOLI (Thales)
Michel BOUVET (GICAT)

SYNTHESE

Issu des réflexions d'un groupe de travail du GICAT, ce rapport est un plaidoyer collectif pour augmenter l'utilisation de l'intelligence artificielle (IA) appliquée aux opérations terrestres. Il couvre les usages opérationnels, les méthodes disponibles et les réponses que l'industrie de défense française doit apporter pour que l'efficacité des forces soit améliorée et que la base industrielle et technologique de défense (BITD) reste compétitive.

D'une part, l'évolution, très rapide ces dernières années, des techniques d'optimisation, des capacités de traitement sur des multiprocesseurs, des capacités de stockage de données ainsi que des méthodes d'apprentissage automatique, ont favorisé le développement significatif de l'intelligence artificielle. Ce rapport explique les différentes approches, méthodes et techniques de l'IA dans une logique aussi vulgarisatrice que possible et tentant de « démythifier » l'IA.

D'autre part, le contexte militaire a profondément évolué : les conflits modernes sont marqués par la densification des menaces, la prolifération de drones à bas coût, l'accélération des boucles OODA et la nécessité d'une supériorité simultanément informationnelle, décisionnelle et opérationnelle.

L'IA n'est plus une option prospective — son déploiement opérationnel est devenu critique.

Partant de quelques exemples capacitaires précis, sont illustrés les possibilités d'utilisation de l'IA, sa valeur ajoutée et les efforts encore à accomplir pour que l'IA soit amenée à son plein potentiel et ainsi améliore encore davantage l'efficacité opérationnelle. Le rapport recense ainsi onze cas d'usage majeurs : détection radar de menaces aériennes, classification optronique, établissement de situation tactique à partir de drones ISR, aide à la décision en environnement secret, réduction de la charge cognitive des opérateurs, véhicules autonomes, aide à la manœuvre, maintenance prédictive, logistique militaire, entraînement par simulation et détection de munitions rôdeuses. Ces applications mobilisent l'ensemble du spectre des paradigmes d'IA — connexionniste, symbolique et générative — selon les niveaux de maturité et les contraintes propres à chaque domaine.

Trois réponses structurantes sont apportées pour faire face aux limites des approches actuelles.

- La première est celle de l'hybridation. Face à l'opacité des systèmes purement connexionnistes et à la fragilité des systèmes purement symboliques, la voie la plus prometteuse réside dans la combinaison des deux. Les approches neuro-symboliques, les *Physics-Informed Neural Networks* (PINNs), qui contraignent l'apprentissage par les lois physiques, et les *Geometry-Informed Neural Networks* (GINNs) illustrent cette convergence. L'IA hybride offre simultanément robustesse, explicabilité, frugalité en données et capacité à respecter des contraintes doctrinales ou réglementaires : autant de propriétés indispensables dans un contexte critique de défense.
- La deuxième porte sur la confiance et la garantie des performances. Après avoir rappelé les six exigences de l'*AI Act* européen, robustesse, efficacité, fiabilité, facilité d'utilisation, transparence et surveillance humaine, ce rapport souligne que ces exigences prennent une forme particulièrement exigeante pour les systèmes de défense. La sûreté peut nécessiter une validation formelle voire une certification ; l'explicabilité en temps réel devient une condition d'acceptabilité opérationnelle ; la cybersécurité, enfin, entretient une relation bilatérale complexe avec l'IA, à la fois vulnérable aux attaques adversariales et levier de détection d'anomalies. Il ne suffit pas qu'un modèle soit précis : il doit être démontrablement robuste, consistant et contrôlable.
- Enfin, la troisième réponse concerne l'intégration et l'appropriation humaine. L'embarquabilité des fonctions IA impose des compromis de compression, de latence et de SWaP (taille, masse, puissance). La qualification doit porter sur le comportement réel du système dans son environnement de déploiement, et non sur un prototype de laboratoire. Par ailleurs, l'appropriation par l'opérateur conditionne l'efficacité réelle des systèmes. L'explicabilité n'est pas un luxe : elle est la condition d'une relation de confiance homme-machine qui permette à l'humain de rester au centre de la décision finale, notamment pour l'usage de la force létale.

En synthèse, ce rapport plaide pour une ingénierie de l'IA de confiance, systémique et souveraine, combinant hybridation des paradigmes, qualification incrémentale, et fédération des acteurs de la BITD autour de méthodologies communes.

Table des matières

1. Introduction

L'évolution, très rapide ces dernières années, des techniques d'optimisation, des capacités de traitement sur des multiprocesseurs, des capacités de stockage de données ainsi que des méthodes d'apprentissage automatique, ont favorisé le développement significatif de l'intelligence artificielle (IA). Rappelons toutefois la définition originelle de l'IA : « un ensemble de théories et de techniques permettant à un système artificiel de simuler l'intelligence ». Les propriétés de l'intelligence recouvrent un large éventail de capacités cognitives permettant de manipuler des données, des informations et des connaissances, comme la perception, l'apprentissage, le raisonnement, la décision, l'action et la connaissance.

IA (Intelligence Artificielle)
Ensemble de techniques permettant à une machine d'accomplir des tâches qui requièrent normalement l'intelligence humaine : percevoir, raisonner, décider, apprendre. L'IA n'est pas un système unique mais une famille de méthodes très diverses (IA symbolique, statistique, générative...). Exemple : un logiciel qui analyse automatiquement des images satellitaires pour détecter des véhicules ou des mouvements de troupes.

1.1. Criticité du besoin

Les opérations terrestres sont aujourd'hui caractérisées par plusieurs types d'exigences : les exigences de supériorité de la donnée, informationnelle et de la connaissance permettant une meilleure planification des actions comme la transparence de l'espace de bataille, le déni d'accès de l'ennemi dans l'ensemble des composantes multi-milieux multi-champs (M2MC), et les exigences pour la supériorité décisionnelle et opérationnelles comme la vitesse des actions, la collaboration multi-entités et multi-milieux, la massification des forces et des effets, l'augmentation de la létalité des ***actions.*** Les enseignements des conflits récents et en cours montrent bien à quel point des systèmes augmentés par des capacités faisant appel à l'intelligence artificielle contribuent à répondre à ces exigences. A tel point qu'un retard pris dans la mise en œuvre de ces capacités peut modifier substantiellement le rapport de forces et changer le sort de la bataille. Ces capacités à base d'IA sont donc aujourd'hui critiques pour disposer d'une supériorité informationnelle, décisionnelle et opérationnelle, dans le contexte aéroterrestre comme dans d'autres milieux.

Leur contribution est distinctive, en effet, dans chacune des dimensions précitées :

- La **transparence** : les solutions d'IA sont plus efficaces que les humains - en nombre limité - pour traiter une masse sans cesse croissante de données hétérogènes issues du champ de bataille. Ainsi, les outils à base d'IA simplifient leur représentation, leur croisement et l'extraction des informations pertinentes, permettant d'établir et de comprendre plus vite et de manière holistique, au sens « qui s'intéresse à son objet dans sa globalité », une situation tactique ou opérative partagée, œuvrant ainsi à lever le brouillard de la guerre, à faciliter l'appréciation de situation, à anticiper et autoriser des manœuvres - défensives ou offensives - efficaces en temps contraint.
- Le **déni** : les systèmes enrichis d'IA accordent aux plateformes individuelles des capacités d'action continue et indépendante des limites physiologiques humaines, y compris lorsqu'aucun humain n'est plus en mesure de les opérer. L'IA est ainsi au fondement d'une capacité nouvelle des vecteurs de renseignement ou de frappe permettant de naviguer et de réaliser des missions dans des conditions de brouillage (GNSS, communications), conditions qui tendent à se généraliser dans la frange de contact comme dans la profondeur adverse.
- La **vitesse** : l'IA contribue à deux titres à l'accélération du tempo sur le champ de bataille. D'une part, elle contribue à l'automatisation de fonctions pour traiter une information et réaliser une action (d'autoprotection, par exemple) en temps réflexe ; d'autre part elle permet -en raison de son aptitude propre à traiter des informations massives- d'accélérer la boucle OODA[1] : perception accélérée de l'environnement, partage automatique de l'information pertinente aux échelons adéquats, simulation et évaluation rapides de scénarios de réponse, activation des effecteurs pertinents en temps critique.
- La **collaboration** : à deux titres également : d'une part, parce que les traitements intégrant de l'IA permettent de simplifier la représentation de l'environnement, et ainsi de partager des informations de nature vectorielle plus légères à transmettre dans un contexte de déni ou de connectivité réduite ; d'autre part, parce que les systèmes logiciels intégrant de l'IA autorisent une autonomisation des plateformes de combat permettant

[1] La boucle OODA "Observer, Orienter, Décider, Agir" est un modèle conceptuel de prise de décision développé par le colonel John Boyd, stratège militaire et pilote de chasse de l'armée de l'air américaine. Ce cadre est conçu pour améliorer l'agilité et l'efficacité dans des environnements dynamiques et incertains.

une collaboration entre machines et ouvrent la porte à de nouveaux effets (systèmes multi-capteurs de surveillance, systèmes coopératifs de défense de zone par exemple).

- La **masse** : l'IA rend possible la démultiplication des traitements des données des capteurs et des actions synchronisées des effecteurs. Sans capacité augmentée par IA, la mise en œuvre de vagues ou d'essaims de drones est limitée par la capacité humaine à gérer un faible nombre de vecteurs en même temps, tandis que l'automatisation et l'augmentation du degré d'autonomie permises par des systèmes intégrant de l'IA permettra à un unique opérateur de gérer une multiplicité de vecteurs en s'adaptant à des situations complexes, non préprogrammées. Le coût humain, matériel et financier d'opérations impliquant une masse d'effecteurs ou une permanence sur zone se trouve ainsi réduit, ce qui élargit l'éventail des options pour le commandement.
- La **létalité**, enfin car l'augmentation par l'IA des moyens du combat permet à la fois de déployer plus de vecteurs attribuables (pour user l'ennemi et rogner son potentiel combattant) et de rendre ces vecteurs plus efficaces, grâce à un ciblage plus rapide, plus précis et/ou systématique, autorisant ainsi une létalité accrue des moyens offensifs (ex., systèmes de ciblage avec assistance par IA) ou une protection renforcée dans un cadre défensif (ex., systèmes de lutte anti-drones). Derrière cette question, se pose celle de la confiance et de la fiabilité du ciblage.
- Enfin, l'IA permet d'améliorer **l'efficacité de la stratégie militaire** qui intègre trois niveaux : stratégique, opératif et tactique, avec des rôles complémentaires pour anticiper et répondre aux menaces, chacun contribuant aux effets recherchés dans un cadre synchronisé, en accélérant la planification, optimisant la pertinence du suivi et la qualité des opérations tactiques

Disposer des compétences fondamentales en intelligence artificielle était déjà fondamental il y a 5 ans, être en mesure de la déployer opérationnellement aujourd'hui devient critique. Le présent rapport s'attachera donc à 1) poser les principes régissant la conception de solutions d'IA ; 2) expliquer leurs usages principaux et en dégager des priorités ; 3) exposer les défis auxquels se heurte aujourd'hui leur mise en œuvre ; 4) proposer des solutions.

1.2. Définitions et vocabulaire

La conception de solutions d'IA repose largement sur l'exploitation de la donnée, de l'information ou de la connaissance. Ces termes doivent donc être définis avant toute chose. Dans la suite du document, nous utiliserons les concepts de "donnée", "information" et "connaissance", définis comme suit (voir Figure 1).

La **donnée** est un élément brut qui n'a pas encore été interprété ni mis en contexte. Il s'agit du résultat direct d'une mesure qui peut être collecté par un outil ou par une personne, ou déjà présent dans une base de données. Les données comprennent donc des données numériques, symboliques, textuelles ou logiques, ainsi que des composants informatiques (codes, exécutables...).

Données structurées
Les données structurées sont organisées selon un format prédéfini et rigide, stockables dans des tableaux où chaque information occupe une colonne identifiée. Elles sont directement exploitables par des outils informatiques classiques. Des classes importantes d'algorithmes d'IA demandent en entrée de telles données (forêts aléatoires...). Exemples : un tableau de gestion des personnels avec des colonnes fixes (grade, unité, date d'affectation, spécialité) ; un historique de maintenance listant pour chaque véhicule la date, le type d'intervention et le technicien responsable.
Données non structurées
Les données non structurées ne suivent pas de format prédéfini simple et ne peuvent pas être rangées de façon pratique dans un tableau. Elles représentent aujourd'hui l'essentiel du volume mondial de données (estimé à plus de 80 %). Leur exploitation requiert des techniques d'IA spécifiques (traitement du langage naturel, vision par ordinateur, etc.). Exemples : comptes rendus opérationnels rédigés en texte libre, flux vidéo de drones, enregistrements audios de communications, photographies aériennes, messages sur réseaux sociaux surveillés dans le cadre d'une veille adversariale.

Une **information** est une donnée intelligible qui prend un sens grâce à une structuration. Une information est donc, par définition, une donnée sémantique pré-interprétée, généralement par un programmeur. En d'autres termes, la mise en contexte d'une donnée crée de la valeur ajoutée pour constituer une information.

La **connaissance** est le résultat d'une réflexion sur les informations analysées. À la différence de l'information, la connaissance peut être partagée et s'appuie sur un référentiel collectif, comme une sémantique métier. Il est d'ailleurs possible d'effectuer des raisonnements logiques de différentes natures sur des connaissances.

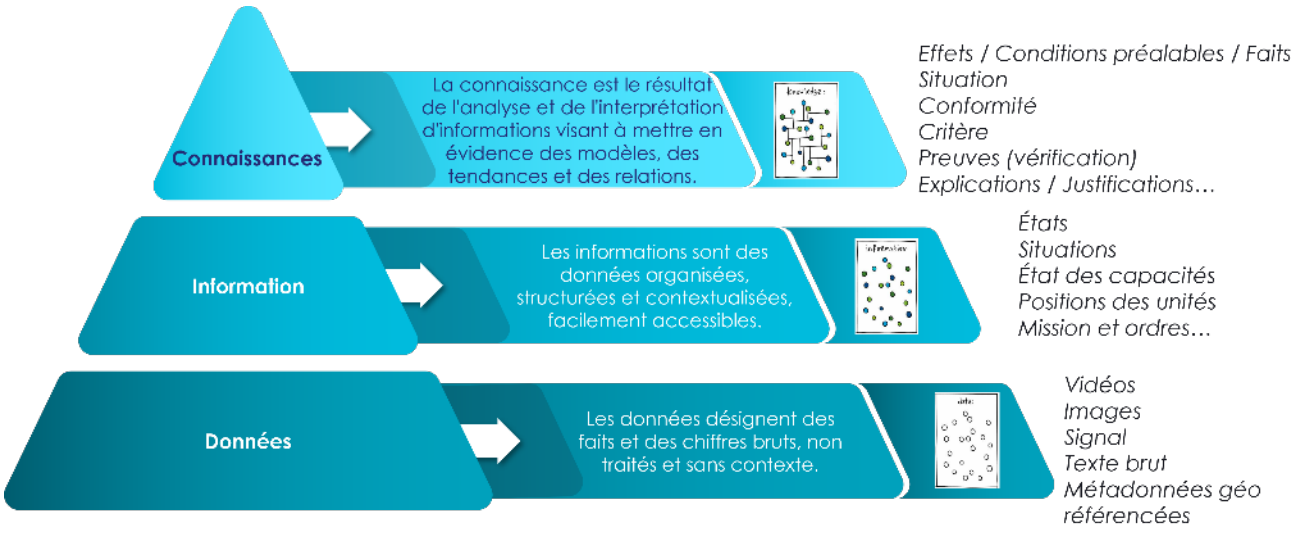


Figure 1 La pyramide donnée/information/connaissance

Toutefois, des informations peuvent être communiquées sans pour autant devenir des connaissances, car leur interprétation finale peut être réalisée par un humain (ce qui est le cas dans la plupart des systèmes de commandement terrestres). Il faut alors les accompagner de leur référentiel, car celui-ci ne sera pas partagé (non implicite). Un ensemble de connaissances est donc en général spécifique à un métier, dont le sens n'est partagé qu'entre les experts du domaine, et correspond à une ontologie et correspond à une ontologie, au sens d'un ensemble structuré de concepts permettant de donner un sens aux informations.

2. Quels usages pour l'IA dans les opérations terrestres ?

La contribution des solutions à base d'IA aux opérations terrestres peut se retrouver dans une variété de systèmes et de capacités. Dès 2019 (voir Figure 2), le ministère des Armées avait identifié les sept capacités prometteuses suivantes : 1) aide à la décision en planification et en conduite, 2) combat collaboratif, 3) cyberdéfense et influence, 4) logistique et maintien en condition opérationnelle, 5) renseignement, 6) robotique et autonomie, et 7) soutien (incluant administration et santé). Celles-ci sont décrites dans le rapport de la Task Force IA de Septembre 2019 intitulé « *L'intelligence artificielle au service de la Défense* ».

Figure 2: Capacités opérationnelles pouvant bénéficier de l'IA

©Rapport MinArm de la Task Force IA de septembre 2019

Nous proposons ici d'illustrer certains de ces cas d'usage particulièrement frappantes et/ou ayant atteint une maturité technique satisfaisante.

Aujourd'hui, le contexte militaire a profondément muté, marqué par une densité et une vélocité inédite des menaces, où les conflits symétriques de haute intensité coexistent avec des engagements asymétriques et hybrides. L'émergence de systèmes bas coût, consommables et perdables (drones, missiles ou engins explosifs improvisés) – souvent assemblés à partir de composants civils – a nivelé les rapports de force, rendant obsolète la supériorité technologique traditionnelle des armées occidentales. Ces outils, déployés en masse, transforment les champs de bataille en espaces saturés, où la guerre des ingénieurs prime : les cycles de développement et de contre-mesures s'accélèrent (quelques mois en Ukraine), exigeant une adaptabilité sans précédent des doctrines et des capacités industrielles.

Parallèlement, certains acteurs s'affranchissent des règles éthiques (ciblage automatisé, attaques indiscriminées), tandis que l'impunité des systèmes autonomes complique l'attribution des responsabilités, brouillant les lignes rouges du droit international. Face à cette perte de contrôle informationnel (brouillage, saturation des capteurs), l'intelligence artificielle émerge comme un palliatif crucial, accélérant les boucles OODA et compensant la désorientation stratégique.

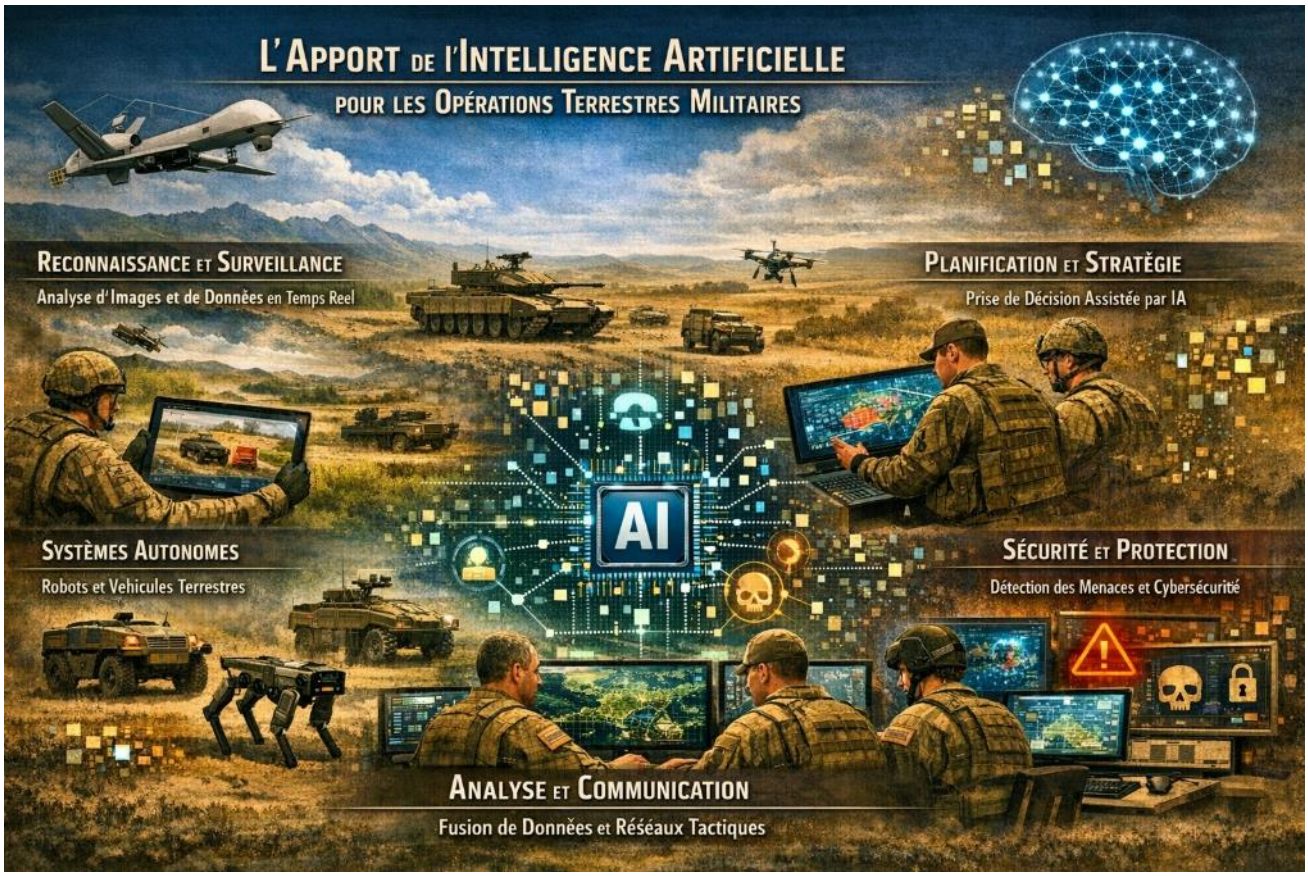


Figure 3: Intelligence artificielle pour les opérations terrestres (image générée par l'IA)

2.1. Détection et identification de menaces aériennes au radar

La détection et l'identification des menaces aériennes sont essentielles pour assurer la sécurité de l'espace aérien. Dans un monde où les menaces évoluent rapidement, il est crucial de pouvoir discriminer simultanément de nombreuses cibles dans des environnements complexes. Les radars de surface et les centres de commandement et de contrôle jouent un rôle clé en fournissant une analyse en temps réel de la situation aérienne, permettant une détection rapide et précise des menaces.

2.1.1. Pour quelles capacités

Les menaces aériennes ont considérablement évolué au fil des années. Les drones, de plus en plus nombreux, et les attaques saturantes représentent, en effet, des défis majeurs pour la sécurité aérienne. Les drones, en particulier, posent des défis uniques en raison de leur petite taille, de leur faible signature radar et de leur capacité à opérer à basse altitude. Les attaques saturantes, où de nombreux objets sont lancés simultanément,

compliquent encore la tâche de détection et d'identification. Les objets furtifs, les hélicoptères dissimulés derrière le relief, les roquettes, les tirs d'artillerie et de mortiers sont autant de menaces qui nécessitent des solutions avancées pour être détectées et neutralisées efficacement.

Les radars de surface sont des outils essentiels pour la détection et l'identification des menaces aériennes. Ils permettent de surveiller de vastes zones géographiques et de fournir des informations précises sur la position, la vitesse et la trajectoire des cibles. Les radars de surface de Thales, par exemple, sont conçus pour détecter des menaces à moyenne et longue portée, allant de 250 km à plus de 500 km. Ces radars sont équipés de logiciels avancés qui prennent en charge les menaces aériennes de nouvelle génération, offrant ainsi une protection accrue contre les drones, les objets furtifs et les autres menaces modernes.

2.1.2. Avec quelle IA et comment elle intervient

L'IA joue un rôle crucial dans la simplification de la prise de décision des opérateurs radars. En imitant la connaissance d'un expert, l'IA statistique et connexionniste permet de traiter des quantités massives de données en temps réel, facilitant ainsi l'identification des menaces potentielles. Par exemple, l'IA peut aider à discriminer un drone parmi divers objets évoluant à basse vitesse, tels que les oiseaux.

Les algorithmes d'apprentissage profond (*deep learning*) sont particulièrement efficaces dans des conditions environnementales défavorables, où la présence de nombreuses détections indésirables peut compliquer la tâche.

2.1.3. Pour quelle valeur ajoutée

Ces algorithmes améliorent la discrimination des drones en se concentrant sur les cibles pertinentes. Cela permet de réduire le nombre de fausses alarmes et d'améliorer la prise de décision en cas de menaces réelles. Ainsi, les algorithmes à base d'IA embarqués dans les radars de Thales sont fiables et explicables, garantissant ainsi une performance optimale dans des situations critiques. Cette technologie permet également de mettre à jour les capacités des radars à distance de manière cyber-sécurisée, assurant une protection continue contre les menaces évolutives.

Figure 4: Détection automatique de cibles par apprentissage profond, intégré à bord de drones

2.1.4. Comment amener la solution à son plein potentiel

Un réseau collaboratif de capteurs fixes, mobiles et aéroportés, permettrait d'assurer une couverture complète et sans angle mort. En effet, la fusion de données issues de différents capteurs –radar, optronique et acoustique– réduirait les fausses alarmes, tandis que l'analyse des signatures micro-Doppler permettrait d'identifier précisément des menaces comme les drones grâce à leurs mouvements caractéristiques. De plus, un lien direct avec les systèmes de contre-mesures, comme les brouilleurs ou les lasers, permettrait une réponse automatisée et rapide une fois une menace confirmée.

2.2. Détection, classification et traitement de menaces en optronique

Face à l'émergence de nouvelles menaces et à leur évolution continue (missiles Face à l'émergence de nouvelles menaces et à leur évolution continue (missiles hypersoniques, drones de combat, essaim de drones...), les capteurs optroniques n'ont jamais revêtu une telle importance pour les forces au combat, nécessitant un niveau de performance exceptionnel. Partant d'un constat similaire, les équipements optroniques répondent à des besoins comparables, dans une sphère du combat plus rapprochée de nos forces. Les équipements optroniques (boules, viseurs, épiscopes) déployés pour la protection de nos moyens terrestres (tels véhicules blindés, postes de commandement) contribuent aussi à accélérer la perception de l'environnement et la détection des menaces, autorisant ainsi des actions d'autoprotection immédiates et le partage en temps réel de la situation tactique.

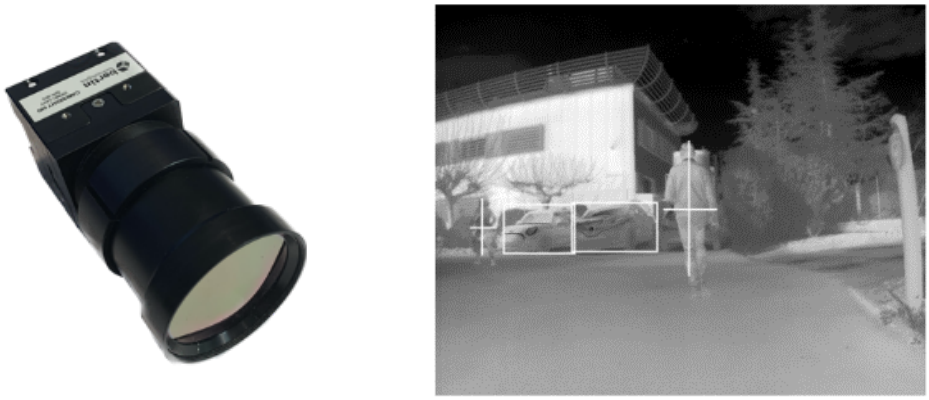


Figure 5 : La CamSight AI de Bertin Technologies est une caméra low-SWaP (Size, Weight and Power) réalisant en temps-réel par IA une reconnaissance et identification de cibles (piétons / véhicules) en imagerie thermique, avec une consommation électrique de l'ordre de 4 W

2.2.1. Pour quelles capacités

Le développement de drones et de munitions téléopérées véloces, avec des vitesses de l'ordre de 400 km/h pour des vecteurs légers, accroît la menace sur nos forces. Ce qui laisse au plus 30 à 45 secondes entre l'apparition d'une menace au-dessus de l'horizon (en zone dégagée) et son éventuelle frappe. La protection de nos forces suppose donc une détection rapide, assortie d'une capacité à discriminer ce qui peut constituer une menace, à l'identifier et à la traiter en temps critique.

Les systèmes optroniques offrent aux forces terrestres débarqués un avantage décisif sur le terrain de jour comme de nuit. Les systèmes optroniques complètent la détection "en avant" opérée par les radars d'une détection "sur place", au plus proche de nos propres moyens. Ces systèmes permettent d'opérer en temps contraint une veille périmétrique et sectorielle des menaces, assortie de capacités de classification et de discrimination en s'appuyant sur des équipements optroniques à longue portée comme les viseurs PASEO ou les boules Euroflir de Safran, ou sur le viseur thermique XTRAIM© pour le décamouflage et ciblage de menaces, les imageurs thermiques portatifs SOPHIE pour la détection et l'identification à longue distance, les jumelles de vision nocturne (JVN) NightRise de Thales.

Figure 6 : Grâce à l'optronique associée aux techniques d'analyse par IA, le combattant bénéficiera à terme d'une assistance avantageuse et précieuse pour la perception de son environnement (@Projet EDA STORE)

2.2.2. Avec quelle IA et comment elle intervient

Les modèles de détection, reconnaissance et identification (DRI) par IA servent à la détection et à la classification d'objets d'intérêt militaire dans un flux de données. Ils récupèrent le flux natif du capteur, le traitent, l'enrichissent de métadonnées et le restituent dans un environnement d'exploitation. Ils peuvent ainsi être placés au service d'un utilisateur humain (dans le cas de capteurs et de systèmes opérés directement par un humain) ou servir comme producteur de données d'entrée pour des briques de cognition et de connaissance situationnelle (pour des systèmes automatisés et/ou autonomes).

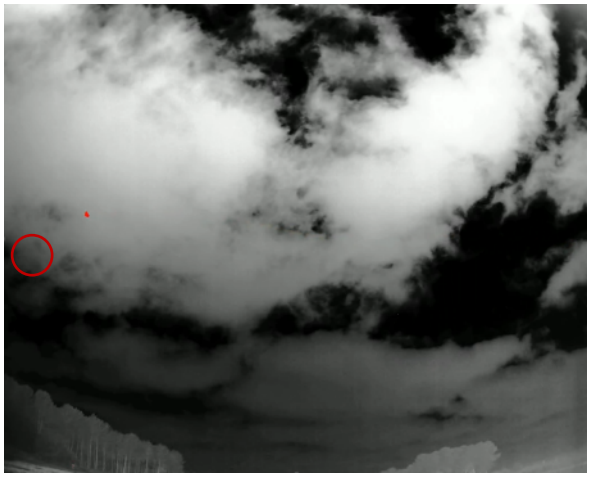


Figure 7 : Bertin Technologies a développé un réseau de neurones de détection précoce de drones aériens, réalisant une détection par IA en temps réel, via l'analyse des anomalies du fond de scène, tout en étant insensible aux perturbateurs en mouvement comme les nuages

Ces modèles sont pour la plupart construits par apprentissage profond (*Deep learning*) sur base d'un corpus de données annotées, et sont intégrés dans des solutions logicielles qui permettent l'ingestion et le traitement automatiques et temps réel de la donnée, puis la restitution des prédictions du modèle dans différentes interfaces possibles : console de l'opérateur capteur, tablette tactique de contrôle d'un drone, interface utilisateur d'un

système de commandement et de contrôle... Ces traitements de bout en bout, combinant IA connexionniste et systèmes experts, s'apparentent donc à des IAs de type neuro-symbolique.

2.2.3. Pour quelle valeur ajoutée

Intégrée aux viseurs PASEO, l'IA joue un rôle d'accélération et de réduction de la charge cognitive pour leurs opérateurs. Elle permet d'assurer la veille panoramique et la levée d'alertes sur détection sans distraction ni lassitude. Elle permet ensuite d'opérer une classification des objets observés, discriminant ainsi la menace entre l'essentiel (un drone, un essaim) et l'accessoire (un vol d'oiseaux). Elle permet enfin d'optimiser l'efficacité de la réponse si les effecteurs assurant l'auto-défense (canons et armes de bord, par exemple) sont asservis sur le viseur longue-portée. En la matière, l'IA apporte un complément et une assistance à l'humain en renforçant la permanence, la célérité et l'efficacité de leurs actions.

Des outils de détection et de classification par IA sur flux optroniques ont déjà été développés par Safran, pour les adapter à ses gammes de viseurs aéroportée et terrestres et assurer dans un premier temps les fonctions de détection et classification, ultérieurement un couplage éventuel des armes sur un tracker automatique.

2.2.4. Comment amener la solution à son plein potentiel

Les solutions d'IA existant pour servir ce type de cas d'usages sont déjà, pour certaines d'entre elles, assez matures. Pour aller plus loin et développer leur plein potentiel, les lignes d'action sont claires :

- Pour faire face à la rareté de la donnée réelle, développer des bases de données étatiques et industrielles et soutenir la recherche sur la frugalité en données des algorithmes ;
- Pour faciliter l'embarquement de ces fonctions dans des vecteurs contraints en taille, en masse et en puissance disponibles, développer des algorithmes frugaux en capacités de calcul et définir des principes partagés (architectures matérielles ;
- Pour faciliter leur déploiement à coûts limités dans une variété de capteurs et de vecteurs, fixer des principes partagés d'intégration aux systèmes et/ou aux IHM (interfaces ou formats d'entrée et de sortie, par exemple).

2.3. Établissement d'une situation tactique à partir de drones ISR

Pour établir une situation tactique (SITAC) à partir de capteurs ISR (*Intelligence, Surveillance, Reconnaissance*) pouvant être embarqués sur des drones et de leurs algorithmes de détection, les équipages sont face à un déluge de données et d'informations qu'il faut fusionner, hiérarchiser, contextualiser pour offrir une réelle capacité de décision rapide tout en permettant à l'homme d'apporter des vérifications. Ainsi cette capacité à représenter de manière complète, exacte et rapide le champ de bataille détermine la pertinence de l'action militaire.

Dans les espaces compartimentés, disputés et déniés qui caractérisent la haute intensité, être en mesure de déployer des moyens de renseignement tactiques et/ou de théâtre résilients et capables est de plus, un facteur de supériorité opérationnelle clair. Il assure la capacité à observer à distance et en permanence afin, soit d'alerter en cas d'anomalie et/ou de menace, soit de capitaliser les informations pour constituer une base de renseignement sur les « patterns-of-life »[2] et les modes opératoires adverses.

2.3.1. Pour quelles capacités

Le déploiement de drones dédiés aux missions d'ISR ou d'ISTAR (ISR + *Target Acquisition*) s'est avéré depuis 20 ans un moyen d'acquérir et de conserver un avantage décisif dans les conflits asymétriques. Sur des théâtres de conflits, l'attrition accrue des vecteurs aériens n'a pourtant pas mis en cause la pertinence de ces moyens ISR pour l'appui au combat aéroterrestre. Une transition s'est juste opérée vers des vecteurs plus légers, moins coûteux, plus versatiles et capables d'opérer dans des situations de déni électromagnétique.

Les systèmes de drones ISR sont désormais en mesure de déployer des capacités d'IA afin de traiter les flux de données générés par leur charge utile. Une variété de solutions existe déjà avec, pour servir leurs besoins (de vol et/ou de mission) une maturité technique encore hétérogène. Il peut s'agir de systèmes de navigation résiliente (basée sur la vision, les anomalies magnétiques...) qui permettent aux drones de poursuivre leur mission en l'absence d'un positionnement fiable par satellite (GNSS : géolocalisation et navigation par un système de satellites). Il peut s'agir de solutions d'IA appliquées à la guerre électromagnétique, qui traitent les données de capteurs radiofréquence et permettent de localiser des émetteurs (radars ou brouilleurs) adverses en croisant par exemple les relevés de goniométrie. Il peut enfin s'agir d'outils de DRI (Détection, Reconnaissance, Identification) par IA qui, comme la famille de solutions ODIN de Safran.AI pour les capteurs

[2] Les « patterns of life » (ou « schémas de vie ») désignent les comportements récurrents et les routines observables d'individus, de groupes ou d'infrastructures (déplacements, routines, communications) afin de détecter des anomalies ou des intentions hostiles.

optiques (visible et IR), traitent -au sol ou à bord- les flux vidéo des capteurs pour détecter et localiser des observables d'intérêt militaire.

Le défis de la masse et le besoin de constante adaptation du matériel au contexte opérationnel réclame des solutions d'opération des essaims versatiles en termes de mission et de plateformes. L'IA joue un rôle crucial dans cette capacité d'adaptation du moyen au contexte. C'est la logique du produit SwarmMaster® développé par Thales qui pourra opérer des essaims de drones différents de façon unifiée pour l'opérateur.

2.3.2. Avec quelle IA et comment elle intervient

S'agissant des fonctions de DRI et de localisation sur les flux de charge utile optronique, les solutions IA qui les assurent sont assez similaires aux solutions évoquées dans le cas d'usage précédent (traitement des flux de capteurs optroniques). Elles intègrent une dimension supplémentaire : la capacité à faire converger les flux traités par IA issus de capteurs multiples pour construire et alimenter une situation tactique partagée, en entrée des systèmes de C2 (aux niveaux tactique ou opératif). Il s'agit de la capacité à fusionner les flux issus de plusieurs voies d'un même capteur (pour des levées de doute ou du déleurrage), de faire converger les vues de capteurs multiples (pour des confirmations ou un affinage de position / de classification), et enfin d'alimenter la situation tactique partagée de ces informations "distillées" avec l'aide de l'IA.

S'agissant des solutions d'IA appliquées aux flux de capteurs électro-magnétiques (ROEM, guerre électronique), le principe est assez similaire. L'enjeu est alors de détecter, identifier et classifier dans le spectre électromagnétique des émissions d'intérêt particulier pour s'y adapter rapidement, afin -par exemple- d'activer certains systèmes : désignation de cibles, activation de contre-mesures, émissions adaptatives... Du point de vue de l'intelligence artificielle et de son intégration logicielle, les principes sont similaires, même si la nature de la donnée de départ diffère. S'agissant des solutions de navigation en déni (navigation basée vision notamment), elles complètent la capacité associée au traitement des flux de charge utile optronique ou électromagnétique, en permettant de se localiser tout instant, y compris lorsque l'intégrité de la connexion au GNSS est compromise. La conception et l'entraînement de solutions de cette nature reposent, dans ce cas également, sur la combinaison de modèles d'IA spécifiquement entraînés à cet effet avec des briques logicielles flexibles, l'ensemble se trouvant *in fine* intégré aux systèmes de mission et de commandes de vol du drone.

L'ensemble de ces briques logicielles élémentaires fait l'objet d'une intégration, qui vise à alimenter la connaissance situationnelle. Pour cela, les modules logiciels et d'IA sont interfacés de telle sorte que leur combinaison fournisse une vue complète, augmentée et adaptative de la situation tactique.

2.3.3. Pour quelle valeur ajoutée

Ces outils ont une double vocation. Pour un vecteur individuel, ils permettent à la fois d'accélérer le ciblage et la boucle renseignement-feux -même dans un environnement électromagnétique dégradé- et de contribuer à un partage de plots pertinents pour établir la situation tactique. Dans le cadre d'un déploiement de vecteurs multiples, ils permettent la tenue de situation collaborative, le déleurrage multi-capteurs, le partage du renseignement d'intérêt opérationnel et l'établissement d'une *Common Operating Picture* qui facilite une décision rapide et appropriée du commandement.

2.3.4. Comment amener la solution à son plein potentiel

Le développement de solutions individuelles (briques élémentaires) progresse rapidement, et s'est largement accéléré au travers de l'industrie depuis 2 ans, en France comme à l'étranger. L'enjeu principal aujourd'hui est de développer des moyens logiciels de faire converger ces solutions pour contribuer à un effet complet pour les systèmes drones et le commandement.

Les travaux engagés en 2025 dans le cadre du Projet Pendragon, qui comprennent une dimension de développement - par l'AMIAD, en lien avec des industriels - d'un C2 pour une unité intégralement dronisée, fondent l'espoir d'un progrès substantiel dans le sens de la création de cette continuité entre les briques élémentaires d'IA et les fonctions systèmes que celles-ci doivent assurer.

La fusion d'information sémantique devient incontournable pour bâtir une situation tactique pertinente et offrir des moyens de construction de cette situation (*sense-making).* Depuis 2006, Thales a développé une approche d'IA hybride qui combine des techniques d'agrégation d'information (données sémantiques) à base IA symbolique comme les graphes conceptuels ou les ontologies capturant les connaissances métier aux approches d'IA connexionniste, permettant ainsi de fusionner les détections et pistes de plusieurs UAV mais aussi de gérer les drones pour assurer la cohérence de la mission (affectation à des tâches de reconnaissance ou de pistage, gestion de la relève des drones...).

Il conviendra toutefois de 1) mener à maturité ce "liant des systèmes" dans le cadre de Pendragon ; 2) permettre à la BITD d'aller plus loin, en se dotant de principes partagés d'architecture, qui permettront à l'ensemble des industriels de développer des systèmes autonomes combinant ces briques dans une perspective d'interopérabilité. De plus, le développement des drones à bas coût, consommables, conduit à alléger les traitements faits à bord et donc à faire les traitements au sol via une station sol C2 réutilisable.

2.4. Prise de décision en environnement secret

Les armées modernes disposent d'une capacité unique de capturer et de transmettre des données, dont le volume augmente de manière exponentielle. Cette abondance d'informations peut être à la fois un atout et un défi. Elle constitue un atout car elle offre une richesse d'informations précieuses pour la prise de décision. Cependant, elle peut également dissimuler les données cruciales dont le commandement a besoin pour prendre des décisions éclairées. En effet, la quantité massive de données peut rendre difficile l'identification des informations les plus pertinentes.

Ainsi les systèmes C2 data-centré avec une architecture permettant d'intégrer de l'IA permet d'accélérer le cycle de la méthode d'élaboration d'une décision opérationnelle tactique (METOD). En effet, l'IA permet d'augmenter la précision de l'analyse de terrain, l'efficacité de la planification d'opération, de l'établissement de plans de ripostes par une optimisation de l'affectation de moyens... Citons, le C2 HexaForce qui se déploie sur des infrastructures des directions des hébergements (DH) basées sur un socle de type ARTEMIS.IA.

2.4.1. Pour quelles capacités

Augmenter le personnel des centres de commandement pour traiter cette masse de données offre des gains limités. Cela impose un compromis entre la quantité d'informations à traiter, la qualité de l'analyse et la rapidité de la prise de décision. Dans ce contexte, l'IA se révèle un soutien clé pour les forces armées. En fusionnant de grandes quantités de données provenant de multiples sources et domaines, l'IA amplifie les capacités humaines. Elle permet une analyse rapide des crises et une prise de décision éclairée, en facilitant l'identification des informations cruciales parmi la masse de données disponibles.

L'IA vise à :

- Réduire le cycle décisionnel de 24 heures à quelques minutes en minimisant les tâches manuelles (préparation des notes, fusion de l'information, recherche, etc.).
- Traiter 100 fois plus d'informations avec le même effectif.
- Accélérer la formation des opérateurs : -30% de temps d'apprentissage.

2.4.2. Pour quels systèmes

ARTEMIS.IA (pour Architecture de Traitement et d'Exploitation Massive de l'Information multi-Sources et d'Intelligence Artificielle) développée par ATHEA[3] vise à offrir une "solution souveraine et sécurisée de traitement massif de données et d'intelligence artificielle". Cette plateforme permettra de "collecter, stocker, croiser, en temps réel et de façon sécurisée" les données provenant de multiples sources et par la même occasion, doter les armées françaises d'une infostructure souveraine de stockage.

ANTICIPE, développé par Thales, est un assistant de prise de décision qui combine la compréhension des données issues de multiples sources hétérogènes et des recommandations collaboratives avec les utilisateurs. Il automatise la gestion des informations critiques (les demandes du commandement et les processus d'informations - CCIR) et des informations prioritaires (PIR). Il utilise également l'IA pour éclairer les décisions humaines dans des contextes incertains.

2.4.3. Pour quelle valeur ajoutée

ANTICIPE a prouvé son efficacité lors de l'exercice OTAN Steadfast Jupiter en octobre 2023, où un QG réduit (10 opérateurs avec ANTICIPE) a rivalisé avec le QG Brunssum (1000 opérateurs). Déployé sur les serveurs OTAN de Mons dans un environnement secret KAST, ANTICIPE a également été retenu par l'ACT OTAN comme cas d'usage pour sa stratégie IA dans le pilier "prise de décision".

2.4.4. Comment amener la solution à son plein potentiel

L'usage de l'IA générative peut être utiliser de rédiger des synthèses pour transmettre la bonne information. Cependant, aujourd'hui ces techniques ne sont pas toujours valides (l'IA générative peut « halluciner »), c'est pourquoi il est important de garantir que la génération automatique de ces synthèses sont opérationnellement correctes.

[3] ATHEA s'appuie sur un ECOSYSTEME de grandes entreprises industrielles et numériques – y compris Capgemini, Sopra Steria Group et Airbus Defense & Space –, mais aussi des ETI, PME, startups, scale-ups, et organismes de recherche spécialisés dans le traitement de données massives et l'IA.

2.5. Prise de décision améliorée et réduction de la charge cognitive

DigitalCrew® est une suite avancée d'algorithmes mise en œuvre par Thales et conçue pour alléger la charge cognitive de l'utilisateur final grâce à la détection, la classification et le suivi automatiques des menaces. Alors que les champs de bataille modernes sont saturés, que les capteurs se complexifient et que les environnements de menace se durcissent, DigitalCrew® aide les opérateurs à traiter les données des capteurs de manière efficace. Cela facilite une prise de décision plus rapide, réduit la charge de travail de l'opérateur et améliore en fin de compte la manœuvrabilité, la survivabilité et la létalité.

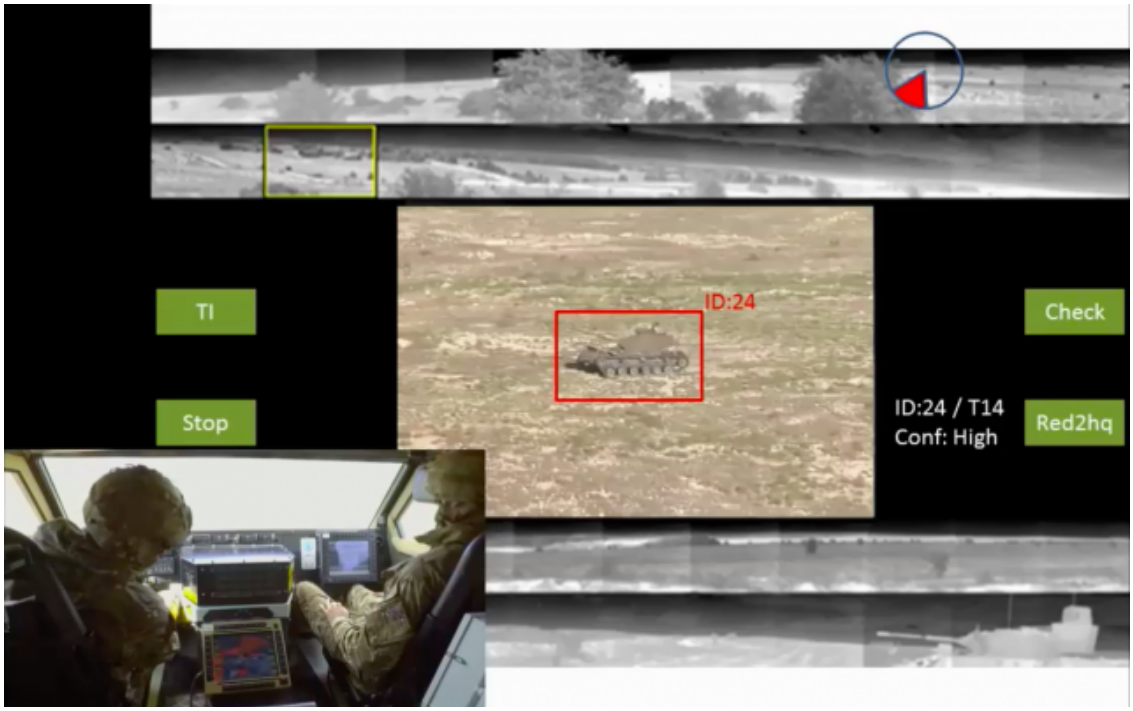


Figure 8 : Une fois relié à un ou plusieurs capteurs EO/IR, DigitalCrew® va réduire la boucle décisionnelle en analysant en continu l'environnement proche et lointain du véhicule.

2.5.1. Pour quelles capacités

Les fonctions d'assistance utilisateur, telles que le suivi d'objets petits et agiles, peuvent être déployées par de simples mises à jour logicielles de la plateforme hôte. DigitalCrew® est polyvalent et indépendant de la plateforme ou du domaine, combinant un ensemble de méthodes traditionnelles et d'apprentissage automatique incluant la détection, le suivi, et la classification d'objets, la combinaison vidéo, la correction des turbulences, ainsi que des outils de support de mission personnalisés, tous destinés à aider les opérateurs dans leurs prises de décisions.

S'appuyant sur plus d'un siècle d'expertise dans la conception de technologies optiques optimisées pour le traitement visuel humain, Thales a maintenant développé les algorithmes DigitalCrew® pour travailler aux côtés des opérateurs humains afin d'interpréter et de traiter les images générées sur le champ de bataille. Contrairement aux opérateurs humains, ce membre d'équipage numérique ne souffre ni de fatigue ni de distraction, et maintient une vigilance constante.

2.5.2. Pour quels systèmes

Véritable exemple d'IA en périphérie, DigitalCrew® s'appuie sur une expertise approfondie en matériel et en intelligence artificielle pour permettre la vision par ordinateur dans certains des environnements les plus difficiles – que ce soit sur terre, sous l'eau ou dans les airs. Ses algorithmes peuvent être directement embarqués sur les capteurs des plateformes, permettant un traitement d'image à faible latence et fournissant des images de la plus haute qualité.

Actuellement, DigitalCrew® est installé sur des plateformes sans pilote de déminage en phase de test. Certains composants sont déjà déployés sur le véhicule britannique Ajax, avec des intégrations prévues prochainement sur le Challenger 3 britannique et le système de visée PAAG de l'équipe conjointe d'appui au feu allemande. De plus, il soutient des applications plus larges de lutte contre les systèmes aériens sans pilote (*Counter-UAS*).

2.5.3. Pour quelle valeur ajoutée

Au-delà des usages militaires, DigitalCrew® est également utilisé dans des contextes civils, tels que la classification d'objets lors d'opérations anti-braconnage menées depuis des avions à voilure fixe au Botswana.

2.5.4. Comment amener la solution à son plein potentiel

Pour améliorer les performances et les capacités de DigitalCrew®, plusieurs axes stratégiques peuvent être explorés, tirant parti de son architecture modulaire et de son intégration avancée d'intelligence artificielle (IA). Tout d'abord, l'optimisation des algorithmes existants constitue une priorité. En exploitant des techniques d'apprentissage de type *deep learning*) plus performantes, comme les réseaux de neurones convolutifs (CNN) ou les *transformers*, il est possible d'améliorer la précision de la détection, du suivi et de la classification des menaces, même dans des environnements complexes ou saturés. L'intégration de mécanismes d'auto-apprentissage continu permettrait également à DigitalCrew® de s'adapter en temps réel aux nouvelles menaces ou aux évolutions des scénarios opérationnels, réduisant ainsi la nécessité d'interventions manuelles pour les mises à jour.

Figure 9 : Robot Phobos développé par KNDS pour les programmes robotiques

2.6. Véhicules automatisés et robotique

L'introduction progressive de ces systèmes permet de projeter la puissance militaire tout en limitant l'exposition des soldats aux dangers, et créer un complément de masse. C'était l'objet du programme FURIOUS, démonstrateur de système autonome multi-plateformes développé par Safran E&D, évalué en 2022, 2023 et 2025 dans des conditions opérationnelles réalistes. C'est aussi l'objet du challenge MOBILEX, piloté par l'AID où le comportement du robot est fortement lié à l'interprétation automatique de son environnement. Le programme DROIDE, mené conjointement par KNDS et Safran E&D, devrait finaliser le développement d'un démonstrateur opérationnel complet.

Figure 9: Robot Véhicule FURIOUS, après une phase de franchissement en autonomie totale durant les essais opérationnels au CENZUB.

L'automatisation des plateformes terrestres constitue une révolution majeure, et de nombreux exemples peuvent être mentionnés, permettant de préserver le capital des forces :

- Robots de reconnaissance : ouverture d'itinéraire, exploration d'environnements hostiles ou contaminés sans risque humain.
- Robots de déminage : localisation et neutralisation de charges improvisées ou de mines.
- Ravitaillement de troupes en traversant des zones dangereuses.
- Systèmes d'armes robotisés : plateformes téléopérées ou semi-autonomes capables d'apporter un soutien feu tout en gardant l'humain dans la boucle décisionnelle.

Le cas d'utilisation exposé ci-dessous concerne le convoyage autonome développé par Arquus :

- Convois logistiques autonomes : réduction des risques pour le personnel lors des missions de ravitaillement dans des zones dangereuses.

Arquus dispose d'une plateforme robotisée téléopérée présentant des avantages de performances, notamment en termes d'agilité et de mobilité. L'enjeu pour Arquus est de doter cette plateforme de briques d'intelligence artificielle permettant à terme de conférer une autonomie au système.

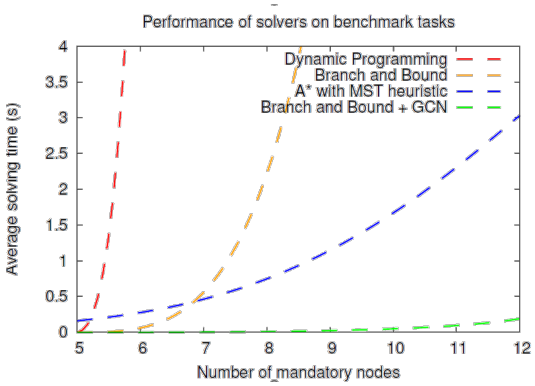
2.6.1. Pour quelles capacités

L'une des fonctionnalités clés à conférer aux plateformes consiste en leur capacité à se déplacer sur le théâtre d'opérations en limitant au maximum les interventions humaines. Cela exige du robot qu'il soit capable de se déplacer sur terrains complexes, non structurés, ou partiellement déstructurés (par opposition aux routes

goudronnées). A ce titre, Arquus travaille notamment sur l'interprétation de l'environnement par ses plateformes robotisées afin de doter ses plateformes d'une fonctionnalité de détection et suivi de chemins.

2.6.2. Avec quelle IA et comment elle intervient

Pour atteindre la capacité souhaitée de suivi de chemins, il s'agit d'entraîner l'IA sur une large banque de données. L'IA mise en œuvre peut s'appuyer sur les réseaux de neurones particulièrement adaptés à l'analyse d'images. Dans une première phase du travail destiné à doter l'IA de la capacité de suivi de chemins souhaitée, Arquus a utilisé une banque de quelques milliers d'images pour entraîner le modèle.



2.6.3. Pour quelle valeur ajoutée

Entraîner l'IA sur une large banque de données suffisante pour permettre de conférer au robot la capacité à suivre un chemin détecté. Ajouté à la capacité d'interprétation de son environnement, le robot peut de se mouvoir de façon autonome sur le terrain semi ou non structuré.

2.6.4. Comment amener la solution à son plein potentiel

Un des axes de travail consiste à étendre la banque de données sur laquelle entraîner l'IA au-delà des quelques milliers de la base de données déjà pratiquée.

Un deuxième axe consiste à améliorer la capacité du robot à interpréter son environnement, notamment en lui permettant d'en inférer la traficabilité (qualité d'un terrain à être traversé par un véhicule donné), condition sine qua non pour se mouvoir sans arrêt ou dommages dans un terrain donné.

2.7. Aide à la conception de la manœuvre

Dans les opérations modernes – qu'il s'agisse d'interventions militaires, de sécurisation de zones sensibles ou de soutien humanitaire – le supériorité tactique repose souvent sur la capacité de plusieurs unités à se déplacer, agir et se coordonner efficacement dans un environnement complexe. Le concept des opérations en réseau, voisin des concepts « *Netcentric Warfare* » (NCW-USA) ou « *Network Enabled Capabilities* » (NEC-UK) met l'accent sur la qualité du partage d'information dans la chaine de commandement, permettant une compréhension commune de la situation et une planification des opérations plus rapides et plus réalistes. Ces concepts ont été de nos jours élargis à la guerre hybride ou multi-domaines.

2.7.1. Pour quelles capacités

Traduire cette vision en actions concrètes nécessite de résoudre des problèmes difficiles : planifier des déplacements, synchroniser des unités très différentes, éviter les conflits d'usage sur le terrain et garantir que certaines actions ne débutent que si d'autres ont été accomplies.

Plusieurs travaux, comme ORTAC (*Operational Ressource and Tactical Action Contro*l) de Safran Electronics and Defense[4], Constraint Programming 2007, évalué en 2012 dans les essais dans le cadre de Phoenix en 2007, 2008, puis à C4ISR-OTM en 2012, iMUGS en 2022 et faisant l'objet d'évolutions récentes} proposent une méthode pour gérer simultanément différents agents tactiques grâce à la programmation par contraintes et des techniques de résolution hybrides. L'environnement est modélisé sous forme de graphe reliant des positions possibles, et les itinéraires des unités sont alors modélisés comme des chemins dans un réseau. Chaque unité tactique, ou agent, doit non seulement trouver un itinéraire possible, mais aussi effectuer des actions à certains endroits, respecter des durées, tenir compte de ses capacités et parfois coopérer avec d'autres unités. La force de l'approche est de réunir ces éléments – mouvement, actions, ressources et coordinations – dans un seul et même modèle, ce qui permet d'obtenir des solutions cohérentes et réalistes.

2.7.2. Avec quelle IA et comment elle intervient

L'une des stratégies évalue "en avant" la recherche sur les différents itinéraires en respectant au mieux les contraintes de coordination. La technique neurosymbolique utilisée permet de trouver plus rapidement des plans réalistes, et parfois même de prouver qu'ils sont optimaux. Les récents travaux, montrent l'intérêt des techniques d'apprentissage à base de graphes permettant de caractériser la structure du problème. Cela permet d'améliorer la résolution, que ce soit à l'aide de réseaux de neurones, ou d'apprentissage symbolique (apprentissage

[4] cf. : Solving Planning and Scheduling Problems in Network based Operations

dynamique de clauses logiques). La figure ci-contre montre la performance obtenue en vert avec une approche hybride neuro-symbolique par rapport aux méthodes classiques, sur un problème réaliste (IROS 2019). D'autres approches ont également montré l'apport de la gestion de contraintes en conflit, dérivées de *Conflict Based Search*. Ces approches allient performances à l'échelle avec une meilleure explicabilité des solutions obtenues.

2.7.3. Pour quelle valeur ajoutée

ORTAC a été évaluée à plusieurs reprises dans le *Battle Lab* en évaluations sur différents scénarios représentatifs : reconnaissance en zone urbaine, renforcement de positions alliées, inspection de sites sensibles ou encore sécurisation de zones humanitaires. Plusieurs travaux adaptent également l'approche à des agents autonomes[5]. Les résultats montrent que la méthode est capable de produire des plans complexes pour plusieurs agents, éventuellement robotisées, tout en respectant les contraintes opérationnelles. Ils démontrent également que certains algorithmes – notamment ceux guidés par des heuristiques et fonctions d'évaluations offrent des gains importants en temps de calcul.

2.8. Maintenance prédictive et maintien en condition opérationnelle

La maintenance prédictive représente bien plus qu'une simple évolution technologique ; elle incarne une transformation profonde de la gestion des systèmes critiques. Traditionnellement, les stratégies de maintenance s'appuyaient soit sur des interventions correctives, déclenchées après une défaillance, soit sur des approches préventives, planifiées selon des calendriers fixes ou des seuils d'usure prédéfinis. Ces méthodes, bien qu'efficaces dans certains contextes, présentent des limites majeures : elles ne tiennent pas toujours compte des conditions réelles d'exploitation ni des variabilités environnementales ou opérationnelles, ce qui peut conduire à des maintenances soit trop précoces, générant des coûts inutiles, soit trop tardives, entraînant des pannes coûteuses et des risques accrus.

2.8.1. Pour quelles capacités

C'est dans ce contexte que la maintenance prédictive émerge comme une capacité stratégique, permettant d'anticiper les défaillances avant qu'elles ne surviennent. Son principe fondamental repose sur la détection précoce des signes de dégradation, même infimes, et sur l'estimation précise du temps restant avant une panne – communément appelé *Remaining Useful Life*. Cette approche ne se contente pas de prédire quand une défaillance pourrait survenir ; elle cherche également à comprendre pourquoi, en identifiant les causes racines des anomalies observées. Ainsi, elle permet de passer d'une logique de réparation à une logique de prévention active, optimisant à la fois la disponibilité des systèmes et les coûts associés à leur entretien.

Cette capacité est particulièrement cruciale dans des secteurs où la fiabilité est non négociable, comme les opérations militaires. En effet, une panne imprévue dans ces domaines peut avoir des conséquences bien plus graves qu'un simple arrêt de production : elle peut mettre en jeu la sécurité des personnes ou la continuité des missions. La maintenance prévisionnelle offre donc une réponse adaptée à ces enjeux, en alignant les interventions sur l'état réel des équipements plutôt que sur des hypothèses théoriques.

2.8.2. Avec quelle IA et comment elle intervient

Pour concrétiser une maintenance prévisionnelle performante, on peut adopter une approche hybride d'IA, combinant les forces de l'IA symbolique et de l'IA connexionniste. L'IA symbolique, fondée sur des modèles formels (comme l'AMDEC ou les arbres de défaillance), exploite des connaissances expertes pour analyser les systèmes critiques bien documentés. Elle permet de modéliser le comportement nominal d'un équipement et de détecter des écarts révélateurs de défauts, en s'appuyant sur des décennies d'expérience opérationnelle. Cette méthode est particulièrement adaptée aux environnements où les mécanismes de dégradation sont maîtrisés, offrant une explicabilité et une rigueur essentielle pour des secteurs réglementés comme l'aéronautique ou la défense.

À l'inverse, l'IA connexionniste excelle dans l'analyse de données massives et complexes, issues de capteurs ou de logs. Les réseaux de neurones identifient des schémas de dégradation dans des séries temporelles, tandis que des techniques comme les chaînes de Markov cachées estiment les états futurs d'un système. Cette approche est idéale pour des systèmes peu documentés, où les données brutes constituent la principale source d'information.

L'hybridation de ces deux IA permet une synergie optimale : les modèles physiques valident les prédictions des algorithmes, tandis que les données enrichissent les règles expertes. Résultat : des solutions adaptables, allant des équipements standardisés aux systèmes dynamiques les plus complexes. Enfin, l'IA générative complète ce dispositif en exploitant les rapports de maintenance pour guider les techniciens et automatiser la rédaction des comptes-rendus, renforçant ainsi l'efficacité globale.

---

[5] projet européen iMUGS, puis PARHERO conduit avec l'ONERA et terminé en 2025

2.8.3. Pour quelle valeur ajoutée

L'adoption de l'IA pour la maintenance prévisionnelle ne se limite pas à une optimisation technique ; elle génère une valeur ajoutée globale, touchant à la fois les aspects économiques, opérationnels et stratégiques.

Sur le plan économique, les gains sont immédiats et mesurables. En évitant les pannes imprévues réduisant significativement les coûts liés aux réparations d'urgence, tout en prolongeant la durée de vie des équipements. Par ailleurs, en optimisant la planification des interventions, elle limite les surstockages de pièces détachées et les interventions inutiles, libérant ainsi des ressources pour des activités à plus forte valeur ajoutée.

Sur le plan opérationnel, la maintenance prédictive à base d'IA améliore considérablement la disponibilité des systèmes. En anticipant les défaillances, elle permet de planifier les arrêts de maintenance pendant des périodes de faible activité, minimisant ainsi l'impact sur les opérations.

2.8.4. Comment amener la solution à son plein potentiel

La maintenance prévisionnelle présente des avantages certains, mais son déploiement à grande échelle est difficile. Le premier défi est la disponibilité, la qualité et l'intégration des données. Les algorithmes d'IA en dépendent. Or, les données sont souvent hétérogènes, bruitées ou stockées dans des systèmes disjoints. De plus, les systèmes actuels ne sont ni prévus pour stocker, ni pour traiter cette donnée. Il est donc nécessaire de faire évoluer ces systèmes et de mettre en place une logistique de la donnée pour capter cette donnée, développer ces approches, intégrer des systèmes d'alertes embarqués et maintenir un apprentissage continu afin d'être toujours fidèles au vécu des systèmes.

Le deuxième défi est la scalabilité des solutions. Les projets pilotes sont souvent très utiles, mais leur généralisation est complexe. Pour y parvenir, il faut adopter une approche modulaire, avec des modèles d'IA réutilisables et adaptables à différents contextes. Par exemple, un algorithme entraîné sur des données de moteurs de chars pourrait être réutilisé pour les véhicules légers, à condition de l'enrichir avec des données spécifiques. Cette stratégie de « *transfer learning* » permet de réduire les coûts et les délais de déploiement.

2.9. Logistique militaire

La logistique militaire est l'ensemble des actions visant à soutenir les opérations des forces armées. Elle se définit comme la science de la planification et de l'exécution des déplacements des forces et de leur maintenance. Elle couvre un large éventail de domaines : acquisition, maintenance et réparation des matériels et équipements ; transport du personnel, des matériels et des équipements ; construction et entretien d'installations ; ravitaillement en combustibles, vivres et munitions ; acquisition ou prestation de services ; soutien médical et sanitaire.

Elle est essentielle pour maintenir la capacité de combat et par conséquent elle est devenue la cible des ennemis notamment grâce aux capacités de frappes dans la profondeur qui augmentent.

De plus, les opérations modernes exigent une logistique capable de s'adapter rapidement aux changements de situation. La flexibilité permet de modifier les objectifs ou de saisir des opportunités, tandis que la résilience garantit la continuité des opérations même en cas de défaillance partielle. Enfin, la nécessité de maintenir une logistique robuste et flexible se confronte à des budgets limités, obligeant les planificateurs à optimiser les ressources.

L'IA révolutionne ainsi la logistique militaire en améliorant la planification, la réactivité et l'efficacité des chaînes d'approvisionnement, facteurs déterminant pour le succès des opérations, tout en réduisant les risques pour les soldats. Ses applications couvrent plusieurs domaines clés, depuis l'optimisation des itinéraires jusqu'au ravitaillement en zone hostile.

2.9.1. Pour quelles capacités

L'IA renforce trois piliers logistiques critiques pour les forces terrestres :

Planification et optimisation des ressources :

- Gestion des stocks et des flux : anticiper les besoins en munitions, carburant, nourriture et matériel médical en temps réel.
- Optimisation des itinéraires : sélectionner les trajets les plus sûrs et efficaces pour les convois, en intégrant des contraintes dynamiques (menaces ennemies, conditions météo, état des infrastructures).
- Coordination multinationale : synchroniser les ressources entre alliés (ex. mutualisation des surplus entre contingents OTAN).

Exécution autonome et robotisée :

- Ravitaillement automatisé : utilisation de véhicules et drones autonomes pour livrer des fournitures en zone hostile, réduisant l'exposition des soldats.

- Évacuation sanitaire robotisée : transport des blessés minimisant le risque pour le personnel médical.
- Maintenance prédictive : surveillance en continu de l'état des équipements (véhicules, armes) pour éviter les pannes critiques.

Résilience et adaptation en temps réel :

- Gestion des crises logistiques : réaction immédiate aux imprévus (ruptures de stock, attaques sur les dépôts, brouillage des communications).
- Fonctionnement en mode dégradé : maintien des capacités opérationnelles même en cas de perte partielle des systèmes IA (ex. retour à des procédures manuelles).
- Cybersécurité proactive : détection et neutralisation des cyber-menaces visant les chaînes logistiques.

2.9.2. Avec quelle IA et comment elle intervient

Pour la **planification logistique**, des algorithmes d'IA connexionniste (apprentissage machine) et d'optimisation analysent des volumes massifs de données historiques et en temps réel. Ils prédisent les besoins futurs en croisant des informations comme l'usure des équipements, les conditions météo ou les mouvements ennemis, puis suggèrent des itinéraires ou des réallocations de ressources optimales. Ces systèmes peuvent, par exemple, identifier qu'un contingent dispose d'un surplus de médicaments tandis qu'une autre unité en manque cruellement, et proposer une redistribution automatique.

Dans le domaine de l'**exécution autonome**, l'IA embarquée dans des véhicules ou des drones prend le relais. Équipés de capteurs avancés (caméras, LiDAR) et d'algorithmes de navigation, ces engins sont capables de se déplacer en terrain hostile, d'éviter les obstacles ou les menaces, et de livrer leur chargement avec une précision extrême, même sous le feu ennemi.

L'IA intervient aussi dans la **maintenance prédictive** : en surveillant en continu l'état des véhicules et des équipements, elle détecte les signes avant-coureurs de pannes et déclenche des alertes pour une intervention avant que le matériel ne tombe en panne, réduisant ainsi les immobilisations intempestives.

Pour garantir la **résilience** et la **cybersécurité**, des réseaux de neurones et des systèmes de détection d'anomalies peuvent être déployés. Ces outils scrutent en permanence les flux de données logistiques pour repérer toute activité suspecte, comme une tentative de piratage ou une falsification d'ordres. Ils simulent également des scénarios de crise (destruction d'un dépôt, brouillage des communications) afin d'évaluer la capacité du système à y faire face et d'ajuster les protocoles en conséquence.

Enfin, des systèmes à base de **décision multicritère** peuvent permettre la résilience et aider à choisir les bonnes configurations des modes dégradés, basculant vers des protocoles de secours si les systèmes principaux sont compromis.

2.9.3. Pour quelle valeur ajoutée

Les bénéfices de l'IA en logistique militaire sont multiples. Sur le plan humain, elle réduit considérablement l'exposition des soldats aux dangers, notamment en limitant leur participation aux convois de ravitaillement, souvent ciblés par l'ennemi. Opérationnellement, elle améliore l'efficacité globale en réduisant les délais de livraison, en optimisant les trajets pour économiser du carburant et en évitant les erreurs de gestion des stocks, comme les surstockages ou les ruptures. Ces gains se traduisent par une meilleure disponibilité des unités en première ligne, qui peuvent se concentrer sur leur mission principale plutôt que sur des problèmes logistiques.

L'IA renforce également la résilience des opérations, en permettant aux forces de maintenir leurs capacités même face à des perturbations majeures, qu'il s'agisse d'une cyberattaque, d'une attaque physique sur un dépôt ou d'une dégradation soudaine des conditions météo. Elle offre enfin un avantage stratégique en facilitant la coordination entre alliés, par exemple au sein de l'OTAN ou de coalitions internationales. De plus, en harmonisant les données logistiques et en proposant des mutualisations de ressources, elle crée une supériorité collective face à des adversaires moins bien équipés.

2.9.4. Comment amener la solution à son plein potentiel

La collaboration (internationale) et la normalisation des standards jouent également un rôle clé. Les armées doivent travailler ensemble pour établir des protocoles communs d'échange de données logistiques, afin d'éviter les incompatibilités entre systèmes. Des partenariats avec le secteur privé, notamment avec des entreprises spécialisées en logistique 4.0 ou en cybersécurité, peuvent accélérer l'innovation et l'adaptation des technologies civiles aux besoins militaires.

2.10. Entraînement et simulation

L'IA transforme également la préparation opérationnelle des forces :

- Environnements virtuels avancés : simulation réaliste des théâtres d'opérations permettant un entraînement immersif.
- Adversaires IA : création d'opposants virtuels capables d'adapter leurs tactiques pour des exercices plus réalistes.
- Analyse de performance : évaluation objective des décisions tactiques et des réactions des soldats pour identifier les axes d'amélioration.
- Ces outils permettent un entraînement plus intensif, plus varié et moins coûteux que les exercices traditionnels sur le terrain.

2.10.1. Pour quelles capacités

Dans un champ de bataille de complexité croissante, avec des actions et effets menés dans différents domaines simultanément, la préparation des missions, l'appréciation des conditions opérationnelles et l'entrainement sont plus difficiles, intensifs et consommatrices de ressources. De plus, la variété et la dynamique des systèmes utilisés ne permettent plus de développer des environnements de simulation monolithiques et figés, que ce soit pour simuler les forces amies ou ennemies. Le projet *Battleverse*, financé dans le cadre d'un budget du Fond Européen de Défense, répond à cette demande des armées de pouvoir préparer des missions, envisager les processus de décisions et simuler des actions opérationnelles tout en couvrant un maximum de scénarios possibles et en envisageant l'utilisation de systèmes variés. Ce projet implique largement les industriels du domaine tels que Thales, Sopra, Safran et Naval Group. Cette capacité doit pouvoir être utilisée aussi bien sur le long terme pour des scénarios fictifs, que sur du court terme avec des situations opératives réalistes.

2.10.2. Avec quelle IA et comment elle intervient

L'approche considérée consiste à pouvoir synthétiser facilement des jumeaux numériques du champs de bataille et des systèmes qui le composent « à la demande ». Le projet envisage la génération des données de scénarios ou de comportements multi-physiques. Dans ce cadre, l'utilisation d'une IA générative neuro-symbolique, permettant d'exprimer et contrôler les modèles physiques est envisagée. Cela permet de pallier au manque de données, informations ou modèles vis-à-vis des objets du champs de bataille.

En complément, le développement des techniques d'IA répond à plusieurs problèmes fondamentaux pour l'application de simulation :

- Le temps utile, avec l'accélération du cycle OODA lors de la planification et de l'exécution des missions. Les techniques d'IA doivent être suffisamment interactives et restituer une information symbolique exploitable immédiatement, sans saturer la charge cognitive.
- L'explicabilité, qui tient compte de l'humain dans la boucle (*in the loop*) ou en supervision (*on the loop*), essentiellement pour la tenue de situation, mais aussi pour le contrôle de l'exécution. La cohérence des informations fournies doit être assurée.
- Adaptation en ligne de l'IA, par exemple en utilisant des techniques de renforcement, afin d'optimiser l'exécution des actions selon le contexte opérationnel, tout en réduisant les marges d'erreur et en considérant des contraintes strictes, par exemple liées aux contraintes d'engagement.

L'ensemble est intégré dans un cadre de simulation militaire flexible, évolutif et à exécution rapide pour réaliser du *wargaming*, du *story-telling* ou de la mise en situation immersive pour les opérations multi-domaines. Les moteurs de simulation doivent être capables de s'adapter à la complexité croissante de la guerre moderne.

2.10.3. Pour quelle valeur ajoutée

La préparation des forces, le tempo des opérations, la prise en compte de l'incertitude et des biais dans l'appréhension du champ de bataille sont autant de préoccupations considérées par ce projet de recherche. La valeur pour la chaine de commandement est donc indéniable, et ce type de jumeau numérique « à la demande » entraine plusieurs avantages :

- Appréhender la problématique à géométrie variable du champ de bataille, l'émergence de systèmes improvisées, en particulier dotés d'autonomie
- Ouvrir le champ des possibles pour l'opérationnel en conception, que ce soit en planification à chaud ou à froid, et tout en permettant l'évaluation des différentes situations d'engagement, et ce sur de très grand nombre de scénarios

- Améliorer l'ingénierie des systèmes en permettant de comprendre leurs usages et leurs appropriations par les forces, notamment pour les systèmes dotés d'IA ou de capacité autonome. Ces environnements de jumeaux numériques peuvent constituer un trait d'union entre les opérationnels et les ingénieurs.
- Bénéficier de la force du « design » génératif permet également d'accélérer le cycle d'ingénierie et d'offrir des boucles conceptions – expérimentations accélérées et plus fluides.

2.10.4. Comment amener la solution à son plein potentiel

Le développement de bibliothèques de modèles, de scénarios et de cas d'usage est le principal axe de capitalisation pour un tel environnement de jumeaux numériques. La capacité à développer de nouvelles IA hybrides, de spécialiser les modèles sur des scénarios concrets et réalistes permet aussi de développer la robustesse des jumeaux numériques. Enfin, la capitalisation sur les données, information et connaissances engendrées par l'environnement génératif permet aussi de palier concrètement à un manque général de données sur la variabilité des opérations futures.

2.11. Détection rapide de munitions rôdeuses pour soft kill

2.11.1. Pour quelles capacités

La détection, même de nuit, de munitions rôdeuses, demande de réagir rapidement à des objets volants qui apparaissent d'abord sous forme de très petits objets, au loin, en venant de n'importe quelle direction (du ciel au ras du sol). Un système d'alerte automatique rapide fondé sur des vidéos infrarouges permet de déclencher à temps un système d'autoprotection soft kill de véhicule blindé, comme par exemple celui de Lacroix Défense. L'IA peut ainsi par exemple encadrer sur l'image infrarouge la zone d'intérêt, pour que l'utilisateur puisse rapidement confirmer l'identification de l'objet et déclencher le système de soft kill.

Figure 10 : Principe de la détection de drones pour la protection par soft kill

2.11.2. Avec quelle IA et comment elle intervient

Les réseaux neuronaux sont particulièrement adaptés à l'analyse d'images, non seulement en lumière naturelle (cas le plus répandu), mais aussi dans l'infrarouge, comme avec la *CamSight* IA de Bertin Technologies.

Intégrer l'IA directement dans la caméra rend son installation plus pratique et confère plus de robustesse au système d'alerte, puisque la surface d'attaque du système de détection est limitée par l'absence de calculateur externe (qui pourrait être lui aussi endommagé).

2.11.3. Pour quelle valeur ajoutée

Les méthodes sans IA sont typiquement fondées sur la détection de changements dans les images (comme un point qui se déplace à l'horizon), ce qui les rend plus sensibles à des situations telles que le mouvement des nuages ou des feuilles des arbres sous le vent. Ces méthodes demandent alors, pour être gérés, des algorithmes plus complexes et plus difficiles à mettre au point.

2.11.4. Comment amener la solution à son plein potentiel

Comme toujours avec l'apprentissage automatique, il est nécessaire d'avoir à disposition des données en quantité suffisante et représentatives des conditions réelles d'utilisation du système de détection de munitions rôdeuses (météo variable, drones aux comportements variés, conditions de roulement variées...). Cela demande un effort d'acquisition d'images typiquement étalé sur la durée et qui doit être suivi d'un sérieux travail d'annotation.

S'assurer d'une rapidité d'analyse des images suffisante est aussi important. Les difficultés viennent du fait que les traitements embarqués sont typiquement contraints en ressource (*SWaP : Seize, Weight and Power*).

3. Quelles méthodes

3.1. Une ou plusieurs disciplines ?

Historiquement, la conception d'algorithmes d'IA émerge dans les années 1950 au travers de deux courants. L'**IA à base de connaissances**, qualifiée aujourd'hui de GOFAI (*Good Old Fashioned AI*) ou d'**IA symbolique**, se base quasi exclusivement sur le raisonnement symbolique et différentes formes de logique.

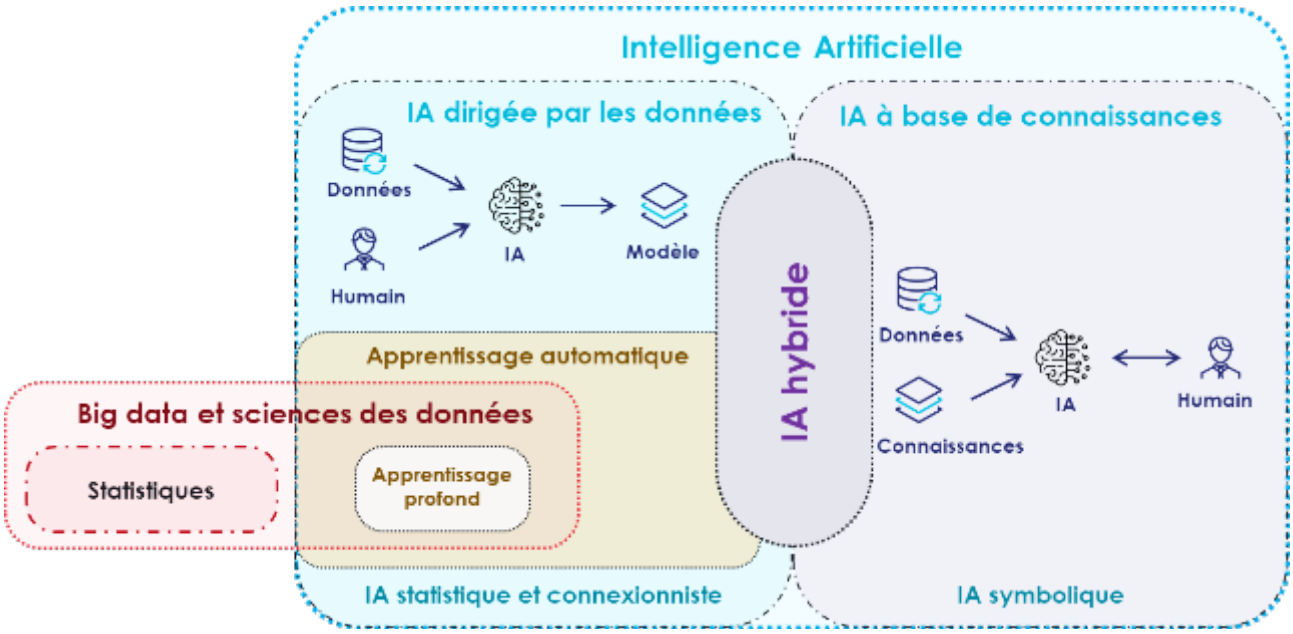


Figure 11: Les principaux paradigmes de l'IA

Elle se distingue de l'**IA dirigée par les données**, également appelée **IA statistiques et connexionniste**, qui est sous le feu des projecteurs ces dernières années, en raison de la collecte massive de données et de l'arrivée de techniques d'apprentissage (comme l'apprentissage profond) ou de l'**IA générative**.

IA symbolique ou à base de connaissances
Approche de l'IA fondée sur la manipulation explicite de règles logiques et de connaissances formalisées par des experts humains. Le raisonnement est transparent et traçable. Exemple : lors de la guerre du Golfe de 1991, le système expert DART (Dynamic Analysis and Replanning Tool) a planifié et replanifié en temps réel le transport logistique de soldats et de matériel. Il a en 4 ans, selon la DARPA, économisé l'équivalent du budget total investi dans l'IA depuis les années 1960.
IA statistiques et connexionniste dite IA dirigée par les données
Approche dans laquelle la machine apprend à partir de grandes quantités de données, en identifiant des corrélations et des régularités statistiques, sans qu'on lui programme

explicitement des règles. L'apprentissage automatique (Machine Learning), une technique majeure d'IA statistique, est entré dans les entreprises vers 2010-2015. Exemple : un algorithme entraîné sur des milliers d'alertes passées pour prédire la probabilité d'une menace en fonction du contexte.
IA *générative*
Sous-famille de l'IA statistique capable de produire de nouveaux contenus (textes, images, sons, vidéos, code...) en s'appuyant sur des modèles entraînés sur de vastes corpus. Exemple : un assistant rédigeant automatiquement un compte rendu d'opération à partir de notes vocales, ou générant un scénario d'entraînement réaliste.

Alors que l'IA symbolique utilise des connaissances transmises à la machine sous forme de modèles pour résoudre des problèmes, l'IA dirigée par les données part d'exemples de solutions qu'elle essaie d'extrapoler par des méthodes statistiques et probabilistes afin de construire un modèle artificiel (cf. Figure 11). Ainsi, leurs domaines d'emploi, leurs usages et leurs objectifs applicatifs diffèrent fortement.

Aujourd'hui, l'IA englobe de nombreuses disciplines, telles que l'apprentissage automatique, la gestion des connaissances, le raisonnement logique, la résolution de problèmes, les systèmes multi-agents, le traitement du langage naturel, la robotique intelligente et les techniques d'inférence probabiliste. La Figure 12 présente la plupart des technologies développées dans le domaine de l'IA selon une approche symbolique ou dirigée par les données.

Apprentissage automatique (Machine Learning)
Technique d'IA où un programme améliore ses performances sur une tâche grâce à des exemples (plutôt qu'en étant programmé manuellement). Cet apprentissage est typiquement fait ponctuellement et produit un système aux performances figées (jusqu'au réentraînement suivant). Exemple : un système de reconnaissance d'empreintes ou de visages associés à des noms, qu'on améliore à partir de nouvelles identifications confirmées
Deep Learning (Apprentissage profond)
Technique d'apprentissage automatique fondée sur des réseaux de neurones artificiels contenant de nombreuses couches de calculs successifs. Cette technique est particulièrement performante pour traiter des données complexes comme les images, le son ou le texte. Exemple : la détection automatique de cibles dans des flux vidéo de drones, ou la transcription de communications radio.

Les techniques probabilistes, basées sur les processus markoviens ou l'inférence bayésienne, sont souvent ignorées, mais sont toujours en développement sous le concept de « *belief state* » (état de croyance). Avec le temps, la partie symbolique s'est structurée en différents domaines connexes, tels que l'inférence logique, la résolution de problèmes ou l'explicabilité.

Inférence probabiliste
Méthode permettant à un système de raisonner sous incertitude : plutôt que de donner une réponse binaire (vrai/faux), il estime la probabilité de différentes hypothèses à partir de données partielles ou ambiguës. Exemple : évaluer la probabilité qu'un convoi observé appartienne à telle force ennemie, en combinant renseignement humain, images et signaux électroniques imparfaits.

Le domaine des systèmes multi-agents, sur lequel se développe actuellement l'agentique, représente l'environnement de construction des architectures d'IA. Rappelons que l'agentique désigne la capacité d'un système, à agir de manière autonome et intelligente, en s'adaptant à son environnement et en prenant des décisions en temps réel. Les agents ont donc un impact sur l'ensemble des technologies développées et influent durablement sur l'état de l'art de l'informatique distribuée s'appuyant sur la communication en réseau. Même si les techniques dites symboliques sont souvent opposées à l'intelligence artificielle connexionniste et probabiliste, de nombreuses approches hybrides émergent. En particulier, l'**agentique** est la forme d'hybridation la plus accessible. Cette approche systématique étend désormais les systèmes agents aux modèles de langage et pousse à l'extrême la combinaison des techniques d'IA.

Systèmes multi-agents
Architecture dans laquelle plusieurs entités autonomes (les "agents") interagissent pour accomplir des objectifs. Les interactions peuvent être coopératives (les agents se coordonnent vers un but commun) ou compétitives (les agents ont des objectifs antagonistes, ce qui peut être exploité pour renforcer leurs capacités mutuelles). Exemples : une flotte de drones autonomes qui se répartissent une zone de reconnaissance sans doublon (coopératif) ; deux agents simulant des forces opposées dans un wargame numérique pour tester des doctrines d'emploi (compétitif).
Agentique (IA agentique)
Désigne des systèmes d'IA capables de poursuivre en décidant eux-mêmes, à chaque étape, quelles actions entreprendre et quels outils mobiliser. À la différence d'un pipeline automatisé aux étapes figées, un système agentique adapte son comportement en fonction des résultats intermédiaires et peut gérer des situations imprévues. En pratique, ces systèmes s'appuient actuellement souvent sur des grands modèles de langage (Large Language Models) qui assure le raisonnement et la prise de décision dynamique. Exemple : un agent auquel on demande de "synthétiser les incidents de sécurité de la semaine" va de lui-même localiser les documents pertinents, en extraire les informations clés, détecter des incohérences et relancer une analyse si nécessaire, sans qu'aucune de ces étapes n'ait été programmée explicitement.

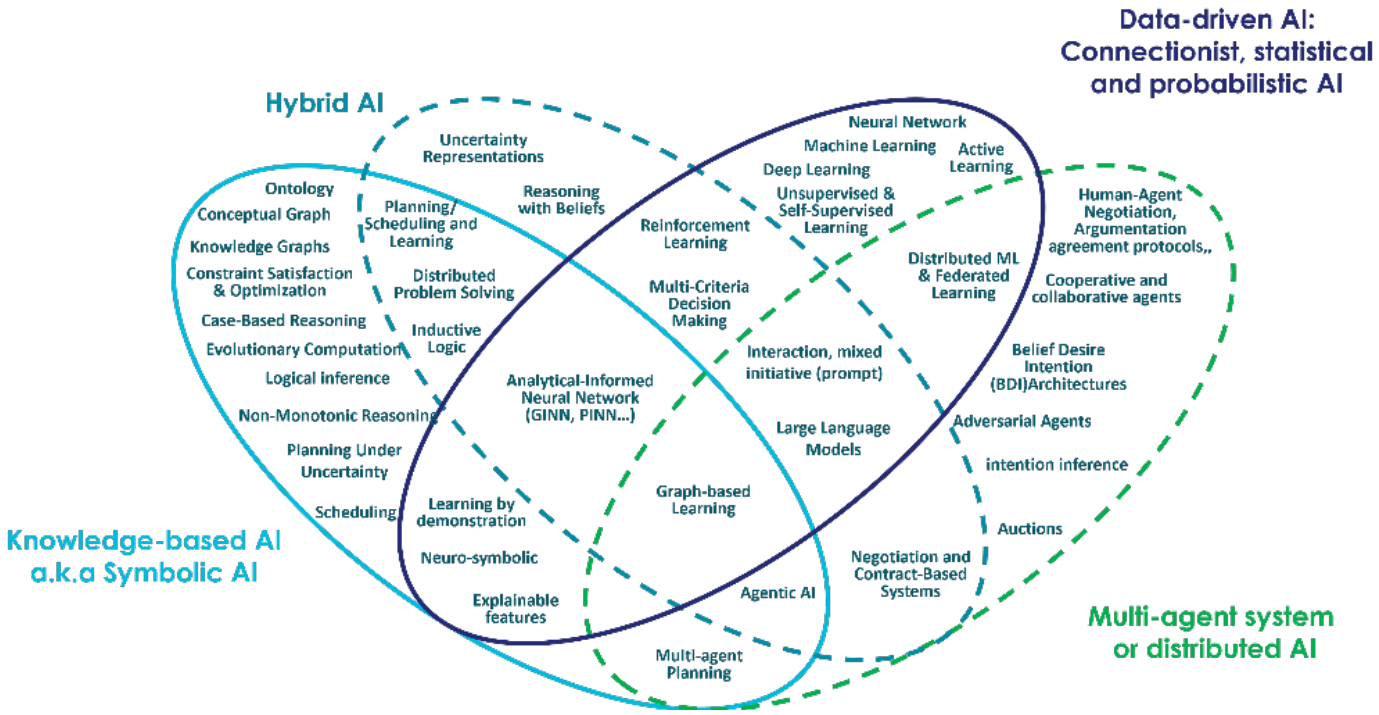


Figure 12 : La zoologie des technologies d'IA

David Sadek, VP "IA et Algorithmique" de Thales, explique que « *L'IA connexionniste est l'IA des sens, et l'IA symbolique est celle du sens* ». C'est pourquoi, pour couvrir l'ensemble des capacités cognitives, l'avenir réside dans l'hybridation des deux approches.

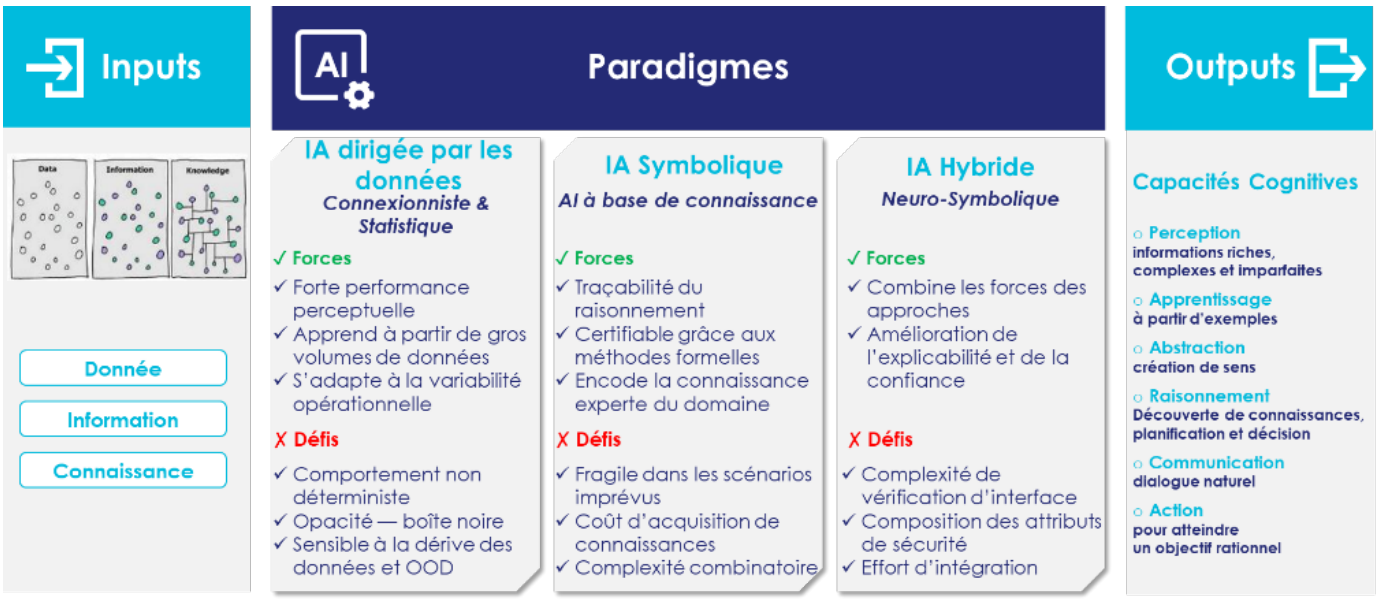


Figure 13: Forces et faiblesses des différents paradigmes en IA

3.1.1. Cartographie de l'IA pour les opérations terrestres

Dans un contexte géopolitique incertain et face à des menaces de plus en plus complexes et asymétriques, l'introduction de l'IA dans les opérations terrestres permet d'accélérer considérablement le rythme des opérations, redéfinissant parfois les paradigmes tactiques, opérationnels et stratégiques.

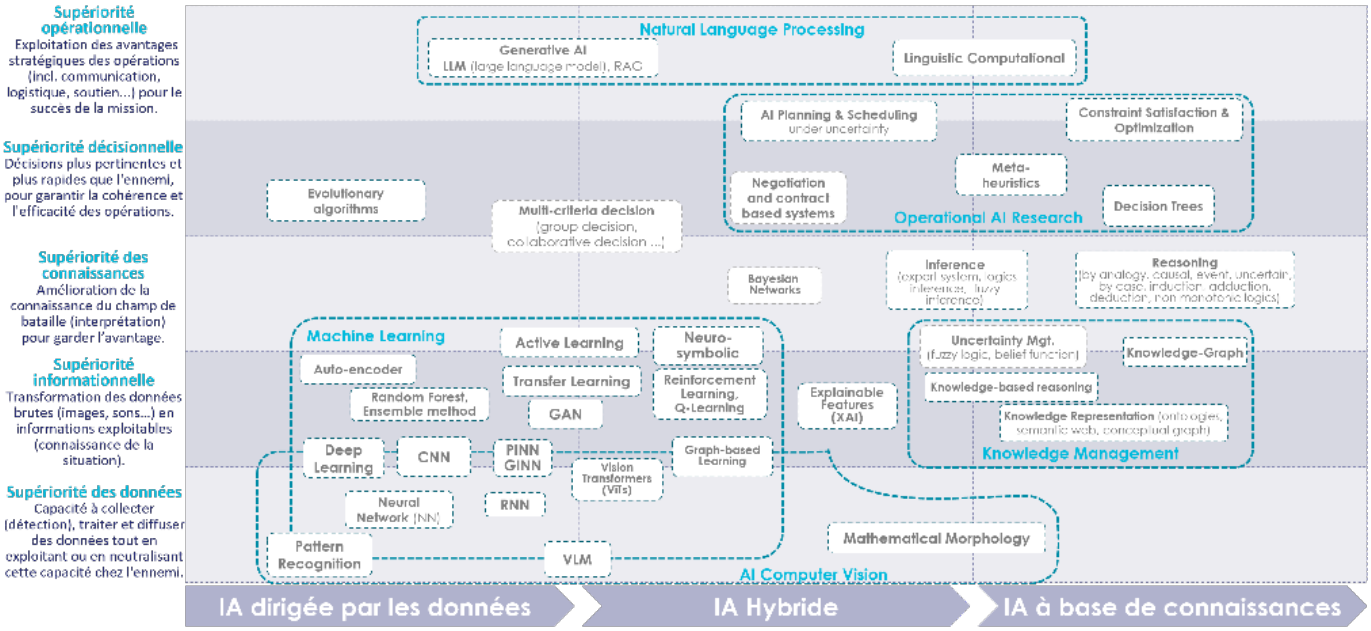


Figure 14 : Les différents paradigmes de l'IA au regard de leurs domaines d'emploi opérationnels

La capacité à traiter rapidement l'information, à prendre des décisions éclairées et à les exécuter sans délai confère un avantage certain au commandement, comme le souligne les cas d'usage décris dans la section 2. La réduction du cycle décisionnel permet de prendre un avantage décisif sur un adversaire technologiquement moins avancé, qui ne peut pas réagir aux évolutions rapides de la situation tactique.

Ce concept initié dans le domaine des opérations en réseaux[6] s'est généralisé et systématisé aujourd'hui à l'ensemble des domaines opérationnels. Il constitue d'ailleurs la base de la guerre hybride moderne ou des

[6] *concept du à David S. Alberts "Network centric warfare: developing and leveraging information superiority"*

opérations multi-domaines (*multi domain operation* - MDO), permettant une coordination planifiée des moyens afin de délivrer des effets synchronisés dans plusieurs domaines. Ce concept précurseur anticipe d'ailleurs de nombreux principes bénéfiques à l'exploitation de l'IA : séparation de la planification et de l'exécution (*i.e.*, conduite) dans un processus continu, flexible et adaptable ; collectif pour la planification et l'exécution, réduction du brouillard de la guerre pour un champ de bataille plus transparent, etc...

Cette approche permet de construire une grille de lecture des capacités apportées par l'IA décrite en Figure 14.

3.1.2. La supériorité de la donnée

La maîtrise de la donnée constitue un atout décisif. Grâce à une collecte massive via des capteurs avancés (satellites, drones, radars), des volumes colossaux d'informations sont générés en temps réel. Leur traitement rapide transforme ces données brutes en renseignements exploitables en quelques secondes (cf. §2.1, et §2.2). Cela permet une prise de décision éclairée, optimisant la planification des opérations, la précision des frappes et l'efficacité logistique. Ainsi, l'intégration de l'IA dans les opérations terrestres ouvre des perspectives majeures, mais son efficacité dépend étroitement de la maîtrise des données et de leur cycle de vie.

Contrairement aux outils logiciels traditionnels, les nouvelles générations de modèles s'appuient sur des calculs statistiques nécessitant des données représentatives, volumineuses et diversifiées pour garantir des prédictions fiables en conditions réelles. Cependant, plusieurs défis persistent, notamment la disponibilité des données d'entraînement et de test, leur adéquation avec les contextes opérationnels (flux de capteurs, ontologies, normes métier), ainsi que leur volume et variété pour couvrir l'ensemble des cas d'usage sans biais.

La souveraineté des données est un enjeu critique, particulièrement pour celles qui sont sensibles comme les images satellites ou militaires, et dont l'annotation renforce encore la valeur stratégique. Leur protection contre les fuites ou les exploitations indésirables impose des cadres stricts de partage, notamment avec les partenaires industriels, tout en clarifiant les droits de propriété intellectuelle et les restrictions d'exportation. Des solutions innovantes, comme le crowdsourcing (exemple ukrainien) ou l'utilisation de données simulées, peuvent compléter les jeux de données réelles, mais elles soulèvent des questions de confidentialité et de licences.

Le réentraînement des modèles pose également un défi majeur, surtout face à l'évolution rapide des contextes opérationnels (comme illustré par le conflit en Ukraine). Il nécessite des méthodologies robustes pour intégrer de nouvelles données terrain tout en maintenant les performances, ainsi que des données de test annotées pour valider quantitativement les modèles sans partager ces ressources avec des tiers. Enfin, la sécurité physique et cyber des données doit être assurée à chaque étape, depuis leur acquisition jusqu'à leur stockage, en passant par leur traitement, afin de préserver l'avantage opérationnel et la confidentialité.

Pour relever ces défis, une collaboration étroite entre « data scientists », opérationnels et industriels est indispensable, afin de définir des procédures adaptées à l'acquisition, l'annotation, le partage et la mise à jour des données, tout en anticipant les risques liés à l'obsolescence ou à la déclassification. L'objectif ultime est de concilier performance des modèles, souveraineté des données et agilité opérationnelle, pour faire de l'IA un levier décisif sur le champ de bataille.

La cybersécurité joue également un rôle clé en protégeant ces flux contre les cybermenaces, préservant ainsi la confidentialité des stratégies et la continuité des missions. Enfin, l'analyse prédictive offre un avantage stratégique majeur : anticiper les mouvements adverses déséquilibre le rapport de force en faveur de celui qui domine l'information. En définitive, la supériorité militaire repose tout d'abord sur la capacité à collecter, analyser et sécuriser la donnée, garantissant réactivité, précision et ascendant tactique sur le terrain.

3.1.3. La supériorité informationnelle

La supériorité informationnelle repose sur la capacité à collecter, traiter et analyser d'immenses volumes de données hétérogènes en temps réel, nécessitant des technologies d'IA particulièrement performantes dans différents domaines :

- L'IA connexionniste et statistique comme l'apprentissage profond et réseaux de neurones est particulièrement adaptés à l'analyse de données non structurées (images satellites, signaux radars, communications interceptées). Ces technologies d'IA dirigée par les données excellent dans la détection et reconnaissance de motifs (pattern) complexes ou la détection d'anomalies dans de grands ensembles de données et d'informations, permettant d'identifier des signaux faibles qui échappent à l'analyse humaine ou aux méthodes statistiques traditionnelles.
- L'IA générative, technologie pertinente pour la fusion des données multimodale car elle permet d'intégrer des informations provenant de sources diverses (images, textes, signaux acoustiques et électromagnétiques) en une représentation cohérente et exploitable. Les modèles génératifs peuvent également combler les lacunes informationnelles en produisant des hypothèses plausibles sur les zones d'ombre du renseignement.
- Les systèmes multi-agents permettent la collecte décentralisée de données et d'informations produits par des réseaux de capteurs intelligents et distribués. Les architectures multi-agents sont particulièrement

robustes face aux perturbations et peuvent maintenir une conscience situationnelle (*situation awareness*) même en cas de dégradation partielle du réseau d'information.

L'intégration de ces technologies dans des architectures hybrides permet une domination du spectre informationnel à tous les niveaux, de la collecte tactique jusqu'à l'analyse stratégique des intentions adverses (cf §2.3). En particulier, les systèmes de surveillance assistés par IA transforment radicalement la reconnaissance du terrain et la détection des menaces :

- Grâce aux techniques d'apprentissage automatique, la détection d'anomalies contribue à l'identification de comportements suspects ou de changements subtils dans l'environnement pouvant indiquer une menace imminente. Ainsi, l'IA dirigée par les données peut ainsi identifier automatiquement les véhicules, installations et mouvements de troupes ennemis à partir d'images aériennes ou satellitaires.
- L'IA hybride reposant sur des combinaisons de modèles physiques ou géométriques avec des techniques neuronales (PINN : *Physics Informed Neural Network* ; GINN : *Geometric Informed Neural Network*) basés sur les données historiques offre des capacités de détection, de reconnaissance mais aussi de prédiction particulièrement robuste, en particulier aux bruits induits par les capteurs.
- La fusion d'information multi-sources (radar, imagerie infrarouge, signaux acoustiques ou électromagnétiques, sources ouvertes), reposant sur des technologies de type graphes de connaissances (réseau sémantiques, graphes conceptuels ou ontologies) ou à base d'IA générative, permet de construire une image opérationnelle enrichie pour une meilleure compréhension de la situation tactique, opérative et stratégique. En effet, cette fusion d'information multi-sources optimise l'efficacité militaire en fournissant une analyse prédictive et une compréhension globale de l'environnement opérationnel.

Toutes ces technologies permettent de construire une meilleure conscience situationnelle, réduisant ainsi le risque d'embuscades ou d'attaques surprises.

3.1.4. La supériorité de la connaissance

La maîtrise des connaissances, alliant données brutes et expertise métier, est un levier stratégique indispensable aux forces armées. Contrairement à une simple accumulation de données et d'informations, la supériorité des connaissances doit intégrer les doctrines militaires, les retours d'expérience (RETEX) et les savoir-faire opérationnels pour transformer les informations comme issues du renseignement en décisions pertinentes et adaptées (cf. §2.4). Une connaissance approfondie des procédures tactiques, des capacités adverses et des environnements opérationnels permet d'affiner les plans, d'anticiper les réactions ennemies et d'ajuster les actions en temps réel.

Cette supériorité réduit les incertitudes et les risques, en s'appuyant non seulement sur des données actualisées, mais aussi sur une compréhension fine des règles d'engagement, des schémas décisionnels et des leçons tirées des conflits passés. Elle optimise également l'emploi des ressources, en alignant les moyens disponibles sur les impératifs doctrinaux et les réalités du terrain. Enfin, elle confère un avantage asymétrique : en combinant renseignement technique (SIGINT, IMINT) et savoir-faire tactique (doctrines OTAN, procédures nationales), une force peut désorienter l'adversaire, exploiter ses faiblesses et maintenir l'initiative.

En effet, manipuler des données ou informations permet de maintenir la cohésion d'une chaîne de commandement ou de gérer la correction et l'intégrité de l'état d'une plateforme (aéronef, navire, robot). Cependant, même s'il est possible d'élaborer des techniques à base d'inférence neuronales, toutes les informations ne sont pas nécessairement sujettes à la manipulation de connaissances. En effet, les taches de raisonnement telles que la déduction, l'induction, l'abduction, la satisfaction de prédicats ou de contraintes doivent reposer sur des sémantiques logiques bien définies (ex. doctrines). Par exemple le problème est flagrant sur l'assistance à la décision pour une chaine de commandement où des logiques temporelles doivent être assurées, bien loin des représentations informationnelles usuelles. Pour bénéficier d'une assistance par IA qui soit plus explicable, il est nécessaire de suivre les enchaînements (*DigitalCrew®,* causalités) logiques et temporels. Évidemment, une explication logique fournie en temps utile permettrait à la chaîne de commandement d'assurer la responsabilité d'une prise de décision difficile. Autre exemple, le comportement d'un robot ou drone autonome doit pouvoir être expliqué à l'opérateur afin d'éviter des interrogations de la part de ce dernier en opération.

Dans tous les cas, disposer d'un cadre automatisé de raisonnement permettra une prise de décision assumée et surtout anticipée par rapport au cycle de décision adverse.

En somme, la supériorité des connaissances – bien au-delà de la simple supériorité informationnelle – fusionne expertise humaine et données structurées pour offrir une capacité décisionnelle supérieure, essentielle à la réussite des opérations militaires contemporaines.

3.1.5. La supériorité décisionnelle

L'un des apports majeurs de l'IA concerne l'amélioration des processus décisionnels. Les systèmes d'aide à la décision basés sur l'IA peuvent traiter des volumes considérables de données en temps réel pour présenter aux commandants une vision claire du champ de bataille et contribuer aux capacités suivantes (cf. §2.5) :

- l’analyse prédictive pour analyser les mouvements ennemis, comprendre leur intention, anticiper leurs actions futures et suggérer des contre-mesures optimales ;
- la planification opérationnelle afin d’évaluer rapidement de multiples scénarios tactiques, pour sélectionner les plans les plus efficaces ;
- la gestion des ressources pour optimiser l'allocation des troupes, véhicules et munitions en fonction des priorités opérationnelles et des contraintes logistiques.

Ces capacités permettent d'accélérer le cycle OODA, donnant un avantage décisif aux forces qui maîtrisent ces technologies.

Cependant la supériorité décisionnelle requiert des capacités de raisonnement complexe, d'anticipation et d'adaptation aux situations inédites, faisant appel à des technologies d'IA différentes mais complémentaires.

- Les technologies de IA symbolique sont alors particulièrement pertinentes pour les domaines où la logique formelle, les contraintes juridiques et doctrinales doivent être rigoureusement respectées. Ces systèmes permettent un raisonnement explicite respectant les doctrines, les règles d'engagement, le droit des conflits armés et les considérations éthiques encadrant l'emploi de la force.
- L’IA hybride représente l'approche la plus prometteuse pour la supériorité décisionnelle en combinant la flexibilité de l'IA dirigée par les données (comme l’apprentissage) avec la rigueur et l'explicabilité des approches symboliques ou à base de connaissances, offrant un équilibre optimal entre adaptation à un contexte dynamique et incertain et le respect des cadres doctrinaux et réglementaires.
- Enfin, la simulation et les jumeaux numériques sont essentiels pour l'anticipation des conséquences des décisions, permettant d'explorer virtuellement de multiples options tactiques et leurs effets probables.

Contrairement aux approches d’IA symbolique de type programmation par contraintes efficaces pour concevoir des plans optimisés sous contraintes de ressources, l'IA générative peut concevoir des schémas manœuvriers entièrement nouveaux adaptés à des situations évoluant dans un avenir dynamique et incertain et ainsi proposer des plans d'opération innovants en explorant des espaces de solutions non conventionnelles.

La complémentarité de ces approches permet de créer des systèmes d'aide à la décision qui amplifient les capacités cognitives des commandants, tout en laissant l'humain au centre du processus décisionnel final.

3.1.6. La supériorité opérationnelle

La supériorité opérationnelle concerne l'exécution optimale des actions sur le terrain, nécessitant des technologies d'IA capables d'opérer en temps réel dans des environnements physiques complexes et dynamiques :

- Particulièrement adapté au contrôle automatisé des plateformes robotisées (cf. §2.6) et à l'optimisation continue des tactiques en fonction des retours du terrain, l’apprentissage par renforcement permet de s'adapter rapidement à des conditions opérationnelles changeantes et améliorer leurs performances au fil des missions.
- Les systèmes multi-agents collaboratifs deviennent incontournables pour les opérations impliquant des essaims de drones ou de robots terrestres, ainsi que pour la coordination entre unités humaines et

robotisées. Ces architectures permettent l'émergence de comportements collectifs sophistiqués à partir de règles locales simples, offrant robustesse et adaptabilité.

- Essentiels pour l'allocation optimale des ressources et la synchronisation des effets multi-domaines en temps réel, les techniques de planification et d'ordonnancement peuvent réajuster constamment les plans d'exécution en fonction de l'évolution de la situation opérationnelle et des opportunités émergentes (cf. §2.3).
- Les outils d'aide à la décision multicritères permettent d'intégrant les dimensions logistiques (cf. §2.9), tactiques, stratégiques et politiques pour une évaluation holistique (au sens qui s'intéresse à son objet dans sa globalité) des options. Ces systèmes peuvent pondérer dynamiquement les différents facteurs selon l'évolution du contexte opérationnel et des priorités du commandement.

3.2. Quelques avantages pour les opérations terrestres

3.2.1. Accélérer le tempo opérationnel

L'introduction de l'IA dans les forces terrestres accélère considérablement le rythme des opérations. La capacité à rapidement traiter l'information, à prendre des décisions éclairées et à optimiser l'action opérationnelle ainsi que les ressources engagées confère un avantage décisif aux forces qui disposent de ces technologies. Cette compression du cycle décisionnel permet de prendre et de conserver l'initiative face à un adversaire moins avancé sur le plan technologique, qui est toujours en retard et incapable de réagir aux évolutions rapides de la situation tactique. Selon l'application et les modes d'action utilisés, plusieurs effets peuvent découler de cette accélération : dissuasion, découragement, surprise, sidération, fulgurance. Cette approche convient aux forces terrestres françaises et permet d'assurer des engagements courts et maîtrisés.

3.2.2. Réduire les pertes humaines

En automatisant les tâches les plus dangereuses et en améliorant la détection précoce des menaces, l'IA permet de limiter significativement l'exposition des soldats et de protéger les forces. Les véhicules autonomes pour la prise de renseignement, la reconnaissance, la surveillance, le transport logistique, les robots de déminage ou les systèmes de détection de tirs (snipers, artillerie) sont autant d'exemples de technologies utilisant l'IA qui préservent la vie des soldats. S'agissant de l'armée de Terre, la maturité des véhicules autonomes progresse actuellement sur deux axes :

- **Robotique terrestre** : l'exposition des personnels est permise grâce notamment au port de charges lourdes et la permanence d'observation. Les besoins en IA stressent les fonctions de perception et de navigation automatique dans des environnements non structurés, déstructurés, ou complexes.
- **Drones aériens** : dotés de bonnes capacités de mobilité dans le milieu aérien (plus facile que le milieu terrestre), les drones sont néanmoins limités par la puissance de calcul et la discrétion de communication. L'IA conférant une autonomie tactique simplifiée, elle permet de sauvegarder les personnels opérateurs en limitant les échanges et assurant les taches de navigation élémentaires.

Par extension, l'IA permet d'automatiser différentes fonctions des engins habités, telles que la guerre électronique de proximité, l'autoprotection, la navigation, ou encore la lutte anti-drones. L'IA apporte également une supériorité de réaction très rapide aux systèmes embarqués et une capacité de détection multi-capteurs. Dans ces systèmes, il est essentiel de pouvoir restituer des informations sémantiques aux humains (opérateurs, utilisateurs, chaîne de commandement), même si l'inférence de bas niveau est purement numérique.

3.2.3. Optimiser des ressources précieuses et limitées

Face à des contraintes budgétaires et à des effectifs souvent limités, l'IA permet d'optimiser l'utilisation des ressources physiques disponibles. Qu'il s'agisse d'optimiser le potentiel capacitaire, de maximiser les effets, de planifier les itinéraires selon différentes métriques (carburant, sûreté, vitesse, etc.), de prioriser les cibles en fonction de leur importance stratégique ou d'optimiser la maintenance des équipements. De telles IAs ont généralement recouru à des résolveurs de contraintes et contribuent à maximiser l'efficacité opérationnelle des forces terrestres. De plus, l'optimisation systématique des ressources du réseau et l'utilisation de capteurs actifs permettent de limiter l'exposition à la guerre électronique.

3.2.4. Adapter le niveau tactique aux environnements complexes et hostiles

Les conflits modernes se déroulent souvent dans des environnements urbains densément peuplés ou des terrains difficiles, non structurés ou déstructurés. L'IA statistique aide les forces terrestres à s'adapter à ces contextes complexes en fournissant des outils d'analyse rapide du terrain, de cartographie en temps réel et d'identification des menaces potentielles. Elle permet d'identifier de manière systématique, rigoureuse et objective les changements de terrain, comme les aménagements, les zones de stockage, les chemins de transit ou les fortifications. De plus, l'IA probabiliste facilite la fusion des informations et permet d'élaborer très

rapidement des hypothèses face à des menaces multiples provenant simultanément de différents domaines (spatial, aéroterrestre, cyber, civil). Pour permettre des prises de décision délibératives (humaines ou automatisées), ces hypothèses doivent impliquer des prédicats sémantiques et des variables symboliques.

3.2.5. Augmenter la subsidiarité, limiter l'isolation et assurer la résilience

Les boucles perception-décision-action s'accélérant fortement (en raison de l'utilisation massive de drones rapides, de techniques de guerre électronique et d'artillerie à grande échelle), le commandement doit responsabiliser au mieux la chaîne au contact en laissant aux échelons inférieurs des capacités d'initiative. Dans un environnement de communication fortement perturbé, le risque d'isolement est élevé, ce qui réduit les capacités de prise de décision classique. En se basant sur la tenue de la situation locale, le recours à l'IA d'assistance ou à des véhicules automatisés permet de maintenir une capacité de combat résiliente, tout en respectant les règles et procédures d'engagement, même en cas de communications fractionnées. Dans ces cas, l'IA compense l'absence de supériorité informationnelle résultant des schémas de communication tactique classiques. L'IA doit ici encore intégrer les connaissances symboliques de la situation tactique et tenir compte de l'intention du commandement.

3.3. La gestion des données et des connaissances

La gestion des données et des connaissances est cruciale pour atteindre la fiabilité et les performances requises. Les outils d'IA dans le domaine de la défense impliquent des briques logicielles basées sur des données et des connaissances, qui doivent être de haute qualité et en quantité suffisante pour concevoir des systèmes performants. Une mauvaise gestion des données, mais aussi des connaissances, peut compromettre la confiance des utilisateurs ainsi que l'efficacité des outils.

Toute politique de gestion des connaissances et des données pertinentes devra relever quelques défis principaux. Trois défis majeurs se dégagent et nécessitent une attention particulière :

- la nécessité de représenter correctement la réalité du terrain, tant dans les données que dans les résultats des algorithmes,
- l'utilisation des retours d'expérience pour améliorer la qualité et la pertinence des résultats des calculs ou des mécanismes de raisonnement, et
- la conception de modèles à partir d'observations imparfaites mais réalistes afin de garantir leur robustesse et leur fiabilité.

La donnée et la connaissance métier qui sous-tendent cette conception, ainsi que la validation et la mise à jour des modèles, doivent faire l'objet d'une gestion prenant en compte une série d'impératifs. Les recommandations proposées ci-après visent à garantir une collecte, une annotation et une utilisation adéquates des données, une capture et une représentation des connaissances, ainsi qu'à explorer les modes de collaboration entre l'industrie et les armées sur ce sujet.

3.3.1. La donnée

Les approches de conception et de mise à jour des modèles d'IA dirigée par les données s'appuient sur des techniques d'apprentissage automatique qui requièrent des données de haute qualité et en quantité suffisante. Les principaux enjeux de la qualité des données sont donc les suivants : la disponibilité et l'adéquation des données, le volume et la variété des données, ainsi que leur fraîcheur et leur sécurité. Les données doivent également être disponibles, pertinentes et adaptées aux besoins opérationnels, avec une structuration et des normes appropriées. Il est donc essentiel de définir une stratégie adaptée à chaque cas d'utilisation, en collaboration entre experts en IA et opérationnels, afin de faciliter la création d'une IA et de prévenir les biais et de garantir la conformité aux exigences opérationnelles.

Les jeux de données doivent être suffisamment volumineux et variés pour garantir la robustesse des modèles. Il est donc recommandé de soutenir des initiatives d'enregistrement et d'annotation de jeux de données réalistes, et de mettre en place des stratégies appropriées, comme le soutien à la génération de données simulées (si elles s'avèrent suffisantes), tout en assurant la sécurité et la fraîcheur des données. Il est alors possible de contrôler les biais d'apprentissage et de rendre les modèles plus robustes. La création de taxonomies partagées et le partage sécurisé des données entre les différents acteurs (étatiques *a minima*, et potentiellement industriels de la BITD) sont également essentiels pour développer des outils d'IA adaptés aux différents métiers. Ces mesures permettront de tirer pleinement parti des possibilités offertes par l'IA pour les opérations terrestres.

Enfin, les modèles peuvent nécessiter des mises à jour avec des données récentes, tout en garantissant la sécurité physique et cyber des données. Il est donc crucial de mettre en place des moyens sécurisés pour mettre les données à disposition et de définir des règles de gestion des modèles afin d'éviter tout risque de régression (notamment dans le cas de réentraînements menés « à la volée » en opérations).

Représenter la réalité du terrain dans les données d'entraînement des modèles

Les algorithmes d'IA doivent répondre à un ou plusieurs besoins métier de leurs utilisateurs. Ils doivent donc être conçus dans la perspective de cet usage. La communication entre les algorithmes et les opérateurs requiert un langage partagé et clairement défini. Pour les modèles intégrant de l'apprentissage automatique, la syntaxe de ce langage est formée par les taxonomies sur lesquelles les modèles sont entraînés et testés. Celles-ci doivent être définies en collaboration entre experts en IA et opérationnels afin de prévenir les biais de données et de garantir la conformité aux exigences opérationnelles. Les taxonomies doivent également être adaptées aux différents cas d'utilisation considérés, en tenant compte des spécificités des opérations terrestres. Elles doivent être régulièrement mises à jour pour refléter les évolutions des besoins opérationnels et des technologies utilisées. Elles doivent également être partagées entre les différents acteurs impliqués dans la conception et la mise en œuvre des modèles d'IA afin de garantir la cohérence et l'interopérabilité des outils développés.

Les données d'entraînement doivent être **représentatives** de la réalité du terrain afin de garantir la performance des modèles. Elles doivent donc être 1°) collectées dans des conditions opérationnelles réelles – à tout le moins en bonne partie – pour refléter les conditions dans lesquelles les modèles seront utilisés ; 2°) annotées de manière précise et cohérente pour garantir la qualité des modèles entraînés, donc par des annotateurs formés au métier ; 3°) validées par des experts métier afin de garantir la pertinence des données d'entraînement et la qualité des annotations ; 4°) stockées et gérées de manière sécurisée afin de garantir la confidentialité et l'intégrité des données ; 5°) accessibles aux différents acteurs impliqués dans la conception et la mise en œuvre des modèles d'IA, afin de permettre l'apprentissage automatique à partir de ces données et garantir la cohérence et l'interopérabilité des outils développés.

Les données d'entraînement doivent également être suffisamment **volumineuses** pour garantir la robustesse des modèles d'IA, qui a besoin de suffisamment d'exemples. Elles devront donc, à ce titre, être 1°) collectées en grande quantité (tout en garantissant leur diversité et leur représentativité) ; 2°) collectées de manière continue afin de garantir, le cas échéant, leur fraîcheur et leur pertinence ; 3°) collectées et annotées de manière semi-automatisée pour garantir la rapidité et l'efficacité de la boucle.

Les données d'entraînement doivent enfin être suffisamment **variées** pour garantir la robustesse des modèles d'IA aux conditions dans lesquelles il leur sera demandé d'opérer. Elles doivent ainsi, à ce titre, être collectées dans des conditions et contextes variés pour garantir leur représentativité et maximiser leur exhaustivité.

D'une manière pratique et générale, il est important que les données soient : 1°) collectées et annotées de manière collaborative afin de garantir la qualité des annotations ; 2°) stockées et gérées de manière centralisée afin de garantir leur accessibilité et leur sécurité ; 3°) partagées entre les différents acteurs impliqués dans la conception et la mise en œuvre des modèles d'IA, afin de mutualiser au mieux les coûts de développement et de rendre les solutions d'IA aussi abordables que possible pour les forces.

Utilisation des données synthétiques

Les observations réelles en conditions opérationnelles sont rares, la donnée manque souvent en quantité comme en qualité. Des approches alternatives peuvent être considérées pour pallier le manque de données, reposant par exemple sur l'utilisation de données synthétiques et/ou de modèles frugaux (i.e. qui ont besoin de moins de données). Il est recommandé, le cas échéant, de financer des projets visant à réaliser des modèles d'IA entraînés sur la base de données synthétiques, d'initier des conventions de partage de données entre nations alliées, et investir dans des méthodes frugales en données.

Les données synthétiques devront quant à elles être 1°) générées de manière réaliste, afin de garantir la pertinence des données simulées à représenter le réel ; 2°) validées par des experts métier, afin de garantir la qualité des modèles entraînés et leur adéquation aux cas d'usage ; 3°) soumises à un examen de leur apport aux capacités prédictives des modèles d'IA dans les cas d'usage opérationnels considérés ; 4°) stockées et gérées de manière sécurisée, afin de garantir la confidentialité et l'intégrité desdits modèles ; 5°) accessibles aux différents acteurs impliqués dans la conception et la mise en œuvre des modèles, afin de promouvoir la cohérence et l'interopérabilité des outils.

Utilisation des retours d'expérience

Les retours d'expérience, quant à eux, seront utilisés pour améliorer la qualité et la pertinence des données d'entraînement. Ils devront donc être 1°) collectés de manière systématique, afin de contrôler la pertinence et la fiabilité des prédictions, ainsi que d'améliorer la performance des modèles d'IA ; 2°) analysés et validés par des experts métier, afin de garantir la pertinence de leur apport aux modèles dans les cas d'usage considérés ; 3°) stockés de manière sécurisée et gérés en versions successives, de telle sorte que les évolutions de modèles auxquelles ils donneront lieu gardent bien trace de leur prise en compte ; 4°) partagés entre les différents acteurs impliqués dans la conception et la mise en œuvre des modèles d'IA, afin de garantir une cohérence des outils développés.

Conception et entraînement de modèles d'IA à partir d'observations imparfaites

Un choix de données d'entraînement et/ou de test inadaptées, car méconnaissant les règles et les connaissances métier ainsi que l'utilisation qui sera faite des briques, peut compromettre la performance des modèles. Une quantité de données insuffisante pour entraîner des modèles performants ou garantir la performance des briques d'IA entraînées dessus, et des connaissances ne couvrant qu'imparfaitement ou pas le domaine d'opérations des briques d'IA, sont autant de défis à relever. Les données d'entraînement doivent donc être adaptées aux besoins opérationnels et présenter toutes les bonnes propriétés citées ci-dessus (quant à la collecte, à l'annotation, au contrôle des annotations, à la validation des jeux de données, à leur stockage et à leur partage).

Pour ce qui concerne les modèles d'IA à proprement parler, ils doivent être conçus et entraînés de manière à garantir leur robustesse et leur fiabilité. Cela supposera qu'ils soient conçus en collaboration entre experts IA et opérationnels, afin de garantir la pertinence et la fiabilité des modèles. Ils doivent ensuite être entraînés sur des données de haute qualité et en quantité suffisante (garantie de robustesse et fiabilité), puis validés par des experts métier (garantie de qualité et d'adéquation au besoin), enfin être stockés et gérés de manière sécurisée (garantie de confidentialité et d'intégrité).

Ils devront également être mis à jour de manière régulière, afin d'assurer leur appropriation à un besoin métier en constante évolution (parce que le contexte ou les menaces évoluent en permanence). Les modèles d'IA doivent être mis à jour en fonction des retours d'expérience du terrain, des évolutions des besoins opérationnels, des évolutions des technologies utilisées. Ces mises à jour devront pouvoir se faire de manière sécurisée, afin de garantir la confidentialité et l'intégrité des modèles.

3.3.2. La connaissance

L'IA symbolique, qui est fondée sur des règles explicites plutôt que sur des prédictions statistiques, représente aujourd'hui l'un des paradigmes les plus prometteurs et controversés dans l'évolution des technologies militaires. Contrairement aux approches d'analyse statistique de données qui dominent actuellement le paysage de l'IA avec leurs réseaux de neurones et plus généralement leurs algorithmes d'apprentissage automatique, l'IA symbolique repose sur la manipulation explicite de symboles et de règles logiques pour représenter et traiter les connaissances. Elle se distingue fondamentalement des autres approches d'IA par sa méthode de représentation et de traitement de l'information. Alors que les systèmes connexionnistes utilisent des représentations distribuées et numériques, l'IA symbolique emploie des structures de données explicites où chaque élément d'information est représenté par des symboles discrets manipulés selon des règles logiques formelles. Cette approche permet une représentation directe des connaissances expertes sous forme de règles conditionnelles, d'ontologies, et de bases de connaissances structurées, organisée en plusieurs grandes familles selon leurs approches et méthodes.

- **Systèmes à base de règles** : Cette famille utilise des règles explicites du type ``si-alors'' pour représenter les connaissances ou l'expertise humaine sous forme de prédicats logiques.
- **Logique et raisonnement automatique** : Cette branche s'appuie sur la logique formelle – propositionnelle, prédicats, logiques modales. Elle inclut les démonstrateurs de théorèmes, les systèmes de résolution logique et les moteurs d'inférence. L'objectif est de déduire de nouvelles connaissances à partir de faits établis.
- **Représentation des connaissances** : Ces systèmes se concentrent sur la structuration et l'organisation des connaissances : ontologies, réseaux sémantiques, frames, graphes conceptuels. Ils visent à capturer la structure des domaines de connaissance de manière formelle et exploitable.
- **Planification automatique** : Cette famille s'attaque à la génération de séquences d'actions pour atteindre des objectifs. Les systèmes de planification classique (STRIPS, PDDL) analysent les états, actions et buts pour construire des plans d'action.
- **Programmation par contraintes (CSP)** : Cette famille modélise les problèmes comme un ensemble de variables, de domaines et de contraintes à satisfaire. Elle inclut :
    - satisfaction de contraintes : recherche de solutions respectant toutes les contraintes (placement, ordonnancement),
    - optimisation sous contraintes : maximiser/minimiser une fonction objectif tout en respectant les contraintes,
    - contraintes temporelles : gestion des relations temporelles entre événements,
    - propagation de contraintes : techniques pour réduire l'espace de recherche. Les solveurs CSP utilisent des algorithmes comme l'arc-consistance, le *backtracking* intelligent, ou les méthodes hybrides.
- **Logique floue et raisonnement approximatif** : Cette branche gère l'incertitude et l'imprécision de manière symbolique :
    - ensembles flous : appartenance d'un élément à un ensemble qui est graduelle plutôt que binaire,
    - règles floues : « si X est approximativement A alors Y est plutôt B »,
    - inférence floue : mécanismes de déduction avec des degrés de vérité,

- systèmes de contrôle flou pour des applications industrielles et robotiques,
- logiques multivaluées : extensions au-delà du vrai/faux classique

On pourrait aussi ajouter le raisonnement probabiliste symbolique (réseaux bayésiens avec variables discrètes, logique probabiliste) qui combine aspects symboliques et gestion de l'incertitude.

Dans le contexte spécifique des opérations terrestres, l'IA symbolique présente des caractéristiques particulièrement adaptées aux défis complexes auxquels font face les forces armées modernes. La nature hautement structurée des mécanismes de raisonnement de cette approche technologique permet une modélisation explicite des doctrines militaires, des règles d'engagement, et des procédures opérationnelles standard, offrant ainsi une transparence décisionnelle souvent absente des systèmes d'IA connexionnistes. Cette transparence devient un enjeu critique lorsqu'il s'agit de systèmes automatisés capables d'influencer directement ou indirectement des décisions tactiques et stratégiques sur le terrain. Ainsi, les règles d'engagement, par exemple, peuvent être directement encodées sous forme de prédicats logiques, permettant au système de raisonner explicitement sur les conditions d'autorisation de l'usage de la force. De même, les doctrines de mouvement et de manœuvre peuvent être formalisées en règles de production qui guident les décisions tactiques en temps réel.

L'architecture typique d'un système d'IA symbolique militaire comprend plusieurs composants interconnectés : une base de connaissances contenant les faits et règles pertinents au domaine d'application, un moteur d'inférence capable de dériver de nouvelles conclusions à partir des connaissances existantes, une interface d'acquisition des connaissances permettant l'intégration de nouveaux éléments doctrinaux, et un système d'explication capable de justifier les décisions prises. Cette dernière composante s'avère particulièrement cruciale dans le contexte militaire où la traçabilité des décisions automatisées est une exigence légale et éthique fondamentale.

Cela dit, les IA non symboliques (fondées sur apprentissage automatique ou par renforcement) peuvent intégrer des contraintes (règles d'engagement, doctrine, etc.), qui peuvent être prises en compte soient de façon graduelle (par une pénalité plus ou moins grande à faire des prédictions qui ne les respectent pas), soit de façon absolue (en détectant avec un système « juge-externe » classique qu'une contrainte est violée, ce qui invalide explicitement la réponse de l'IA, comme par exemple en interdisant à un drone marin de sortir d'un certain périmètre).

Représentation des connaissances

Les systèmes à base de connaissances, qui constituent la manifestation la plus mature de l'IA symbolique, trouvent dans le domaine militaire des applications naturelles. Ils peuvent encapsuler l'expertise de commandants expérimentés sous forme de règles heuristiques, permettant ainsi la diffusion et la standardisation des meilleures pratiques tactiques. Cependant, la construction de telles bases de connaissances requiert un processus de maïeutique complexe et coûteux, nécessitant une collaboration étroite entre experts du domaine militaire et ingénieurs de la connaissance.

Le premier défi majeur réside dans la transformation des connaissances humaines en représentations symboliques exploitables par la machine. L'expertise militaire terrestre est souvent tacite, acquise par l'expérience plutôt que par l'apprentissage explicite de règles. L'extraction et la formalisation de cette expertise sous forme de règles symboliques nécessitent un processus long et coûteux, impliquant des experts du domaine qui peuvent avoir des difficultés à articuler explicitement leur savoir-faire. De plus, cette expertise évolue constamment en fonction des nouvelles menaces, technologies et leçons apprises, nécessitant une mise à jour continue des bases de connaissances.

L'enjeu de la complétude est particulièrement critique. Il est pratiquement impossible de représenter exhaustivement toutes les connaissances d'un domaine opérationnel, surtout quand celui-ci évolue. Les systèmes d'IA à base de connaissances fonctionnent dans des ``mondes fermés'' où ce qui n'est pas explicitement représenté est considéré comme faux ou inexistant. Cette limitation peut conduire à des raisonnements incorrects face à des situations non anticipées. De plus, l'imperfection de l'information représentent des défis particulièrement aigus dans l'environnement militaire. Ces systèmes d'IA symbolique traditionnels ont des difficultés à gérer efficacement les situations où l'information disponible est partielle, contradictoire, ou douteuse. Bien que des extensions comme la logique floue, les réseaux bayésiens ou les systèmes de raisonnement probabiliste peuvent pallier ces limitations, leur intégration complexifie significativement l'architecture des systèmes et peut compromettre leur transparence.

Enfin, le biais de modélisation est omniprésent dans les systèmes symboliques. Chaque choix de représentation reflète une vision particulière du monde. En effet, les connaissances formalisées portent inévitablement l'empreinte cognitive et culturelle de leurs sources. De plus, le passage du langage naturel aux représentations logiques implique des choix interprétatifs.

Maintenance et complexité

Les bases de connaissances souffrent souvent de problèmes de maintenance. Ajouter de nouvelles connaissances (règles métiers, contraintes opérationnelles...) peut créer des incohérences avec l'existant.

Selon la technologie employée, l'explosion combinatoire peut limiter le passage à l'échelle. Ainsi, les systèmes à base d'IA symbolique peuvent rapidement devenir ingérables lorsque la base de connaissances atteint une taille critique, entraînant des problèmes de performance et de cohérence. Dans le contexte militaire, où les situations peuvent nécessiter la prise en compte simultanée de multiples facteurs (terrain, météo, ennemi, forces propres, mission, temps disponible), la complexité combinatoire peut rapidement dépasser les capacités de traitement en temps réel. Cependant, des approches de type CSP ont un comportement inverse.

3.3.3. Vulnérabilités des IA

Les attaques adversariales[7] représentent une menace aux systèmes d'IA. Avec les IA symboliques, un adversaire ayant accès aux règles et à la structure logique du système peut potentiellement concevoir des inputs spécifiquement conçus pour exploiter les failles ou limitations du raisonnement symbolique. Ces attaques peuvent être particulièrement sophistiquées car elles exploitent la logique même du système plutôt que ses vulnérabilités techniques traditionnelles. Les réseaux de neurones subissent aussi ce genre d'attaque (un panneau de signalisation un peu modifié peut faire échouer une voiture autonome, par exemple).

L'empoisonnement des bases de connaissances des IA symboliques constitue un autre vecteur d'attaque critique. Si un adversaire parvient à introduire de fausses informations ou des règles malveillantes dans la base de connaissances d'un système d'IA symbolique, il peut influencer de manière subtile mais significative les décisions prises par le système. Cette forme d'attaque est particulièrement insidieuse car elle peut rester non détectée pendant de longues périodes tout en compromettant progressivement l'efficacité opérationnelle. La situation est similaire à l'empoisonnement des bases de données servant à entraîner les IA d'apprentissage automatique.

La dépendance aux infrastructures de communication expose également ces systèmes aux attaques de déni de service et d'interception. Les systèmes d'IA symbolique militaires existants nécessitent souvent des échanges d'informations en temps réel avec des sources multiples (satellites, drones, capteurs au sol, bases de données centralisées). La disruption de ces flux d'information peut sérieusement compromettre la performance des systèmes, voire les rendre dangereux en les forçant à opérer avec des informations obsolètes ou incomplètes. Ce vecteur d'attaque est bien sûr aussi pertinent pour des IA non symboliques qui utiliseraient ces mêmes canaux d'information.

Les bases de connaissances symboliques soulèvent plus nettement des enjeux de protection des données sensibles. Même sans accès direct aux données, un système à base de connaissances peut déduire des informations sensibles par raisonnement. Des règles apparemment anodines peuvent révéler des corrélations permettant d'inférer des informations classifiées. De plus, la transparence des systèmes symboliques, souvent présentée comme un avantage, peut devenir dans certains cas problématiques car cette capacité à expliquer un raisonnement peut exposer des informations confidentielles. Enfin, la combinaison de plusieurs bases de connaissances peut créer des inférences non anticipées, révélant des informations sensibles par croisement.

4. Quelles réponses

4.1. Hybridation

Approches hybrides
Combinaison de plusieurs méthodes d'IA (par exemple IA symbolique et IA statistique) éventuellement avec d'autres approches (mathématiques, physiques) pour tirer parti des avantages de chacune d'entre elles comme la puissance de traitement des données de l'IA statistique et la transparence, la traçabilité du raisonnement de l'IA symbolique, la connaissance de la physique ou de propriétés mathématiques telles que l'invariance par rotation. Exemple : un système de commandement assisté qui utilise le deep learning pour analyser des images, puis applique des règles d'engagement formalisées pour proposer une décision conforme au droit.

Aujourd'hui, les défis induits par l'IA dirigée par les données et l'IA à base de connaissance prennent une nouvelle dimension avec l'IA hybride et plus particulièrement l'émergence des approches neuro-symboliques qui tentent de combiner l'apprentissage automatique et le raisonnement symbolique, cherchant à bénéficier des avantages de chaque paradigme tout en atténuant leurs limitations respectives. Les systèmes futurs combineront

[7] Une attaque adversariale consiste à ajouter une petite perturbation imperceptible à une entrée pour modifier la sortie d'un modèle d'apprentissage automatique, comme altérer la classification d'une image

probablement les avantages de l'IA symbolique (transparence, explicabilité, conformité doctrinale) avec ceux des approches connexionnistes (capacité d'apprentissage, robustesse au bruit, généralisation). Cette convergence pourrait permettre de surmonter certaines limitations actuelles tout en préservant les bénéfices spécifiques de chaque approche.

4.1.1. Physics-Informed Neural Networks

La nouvelle classe de réseaux de neurones "Physics-Informed Neural Networks" (PINNs) repose sur une hybridation avec des modèles physiques. Ces réseaux neuronaux sont entrainés pour résoudre des tâches d'apprentissage supervisé tout en respectant toutes les lois de la physique décrites par des équations différentielles qui limitent l'espace des solutions admissibles par le réseau de neurones lors de la phase d'apprentissage. Les lois physiques pouvant être intégrées dans ces PINNs sont très diverses et vont de la mécanique des fluides (équations de Navier-Stokes) à l'électromagnétisme (équations de Maxwell) en passant par la thermique (équations de Fourrier). Plus généralement, toute loi physique sous forme d'équations différentielles peut être capturée par un PINN. Même si cette nouvelle technologie n'a pas encore atteint sa maturité technologique (faible TRL), elle va avoir dans les prochaines années des applications importantes dans de nombreux domaines comme l'aéronautique ou la défense au travers par exemple des jumeaux numériques.

4.1.2. Geometry-Informed Neural Networks

La géométrie de l'Information est devenue un outil très populaire en IA, en particulier chez les GAFAMI (Google, Amazon, Facebook, Apple, Microsoft, IBM) qui utilisent le gradient associé à la métrique de Fisher pour prendre en compte la structure géométrique de l'espace des paramètres des réseaux multicouches. Des premières preuves de concepts de « *Geometric-Informed Neural Networks* » (GINNs) ont été mises en œuvre pour des fonctions comme l'ATDR (*Automatic Target Detection and Recognition*) sur les signatures micro-Doppler ou cinématiques des cibles ou sur de la reconnaissance d'images à partir de caméras 360° fisheyes.

4.1.3. Deep Morphological Network

Les réseaux de neurones convolutionnels (CNN – *Convolutional Neural Networks*) se sont montrés efficaces pour la classification d'objets dans les images. Cependant dans certains cas, les CNNs n'ont pas une bonne performance notamment en termes d'interprétation géométrique. Pour surmonter ce problème, on utilise des opérations non linéaires, telles que les opérations morphologiques. En effet, la morphologie mathématique consiste à analyser une image par le prisme d'un élément structurant dont on maitrise sa topologie ou sa géométrie et cela grâce à des opérations ensemblistes élémentaires (érosion, dilatation, ouverture, fermeture, gradient morphologique...). Cette technique d'IA à base de connaissances (capturées par l'élément structurant) permet de transformer progressivement l'image pour en faire ressortir les éléments d'intérêt. Son hybridation avec les réseaux de neurones a été appliquée à la reconnaissance de formes dès 1991 mais ces dernières années, une nouvelle architecture neuronale est apparue : *Deep Morphological Network* (*DeepMorphNet*). Les convolutions sont ici remplacées par des filtres morphologiques capable d'effectuer des opérations non linéaires tout en effectuant le processus d'apprentissage des caractéristiques sous-jacentes aux éléments structurants. Ces *DeepMorphNets* peuvent ainsi modéliser les relations spatiales d'un objet d'intérêt ou apprendre la structure d'une image.

4.1.4. Inférence floue

Des combinaisons plus exotiques d'IA peuvent être mise en œuvre. Citons les systèmes symboliques flous qui intègrent la logique floue et les systèmes à base de connaissances. Ces systèmes sont une extension des systèmes à base de règles, dans lesquels on ajoute la possibilité de représenter des règles floues et de les manipuler à travers des mécanismes d'inférence floue. Les systèmes neuro-symbolique-génétiques sont quant à eux, composés d'un algorithme génétique responsable de l'acquisition de connaissances à partir des données (apprentissage), et d'un module symbolique responsable du moteur d'inférence symbolique (raisonnement). Dans cette mouvance, le module *Alpha* de la start-up américaine Psibernetix (acquise en 2019 par Thales) devenue célèbre pour avoir tenu en échec des pilotes de chasse chevronnés dans des simulations de combat aérien, repose sur une combinaison de logique floue, d'arbre de décision et d'algorithmes génétiques, permettant ainsi une certaine résilience au bruit, aux incertitudes environnementales et aux aléas divers.

4.1.5. Les atouts de l'IA hybride

L'intelligence artificielle hybride connaît une impressionnante expansion, nourrie par de formidables promesses comme la robustesse, l'explicabilité, la frugalité ou son usage pour la décision collaborative.

Si chaque forme de supériorité bénéficie de technologies d'IA spécifiques, l'avantage décisif provient de leur intégration dans des architectures adaptées aux besoins spécifiques et souvent hybrides couvrant l'ensemble du spectre informationnel, décisionnel et opérationnel :

- combinant différentes approches d'IA à travers les échelons tactiques, opératifs et stratégiques, les systèmes cognitifs hiérarchiques permettent une cohérence décisionnelle verticale tout en préservant l'autonomie adaptative au niveau local ;
- intégrant les différentes technologies spécialisées pour coordonner des effets à travers les domaines physiques et informationnels, ces systèmes d'IA permettent une synchronisation précise des actions dans les dimensions terrestre, aérienne, électromagnétique et informationnelle.

Cette approche holistique de l'hybridation des technologies d'IA (symbolique, connexionniste et générative) constitue la voie la plus prometteuse pour développer une supériorité militaire durable dans les conflits contemporains et futurs, où les dimensions informationnelle, décisionnelle et opérationnelle sont indissociablement liées.

4.2. IA de confiance et garantie des performances

Rappelons que selon la nouvelle réglementation européenne, l'IA Act, un système à base d'IA est digne de confiance s'il répond à six exigences de haut niveau : robustesse, efficacité, fiabilité (y compris la sûreté et la sécurité), utilisabilité, interaction humain-système (incluant la transparence, l'explicabilité et l'interopérabilité) et contrôle humain (y compris les questions éthiques).

IA de confiance (Trustworthy AI)
IA conçue pour être fiable, explicable, robuste, éthique et contrôlable par ses opérateurs humains. En contexte militaire, cela implique notamment la traçabilité des décisions, la résistance aux manipulations adverses et le respect des règles d'engagement. Exemple : un système d'aide à la décision qui indique non seulement sa recommandation, mais aussi son niveau de confiance, les données utilisées et les limites de son raisonnement.

Ainsi les caractéristiques de l'IA digne de confiance se définissent comme suit.

- La **robustesse** offrant la capacité du système à réaliser la fonction prévue en présence d'entrées anormales ou inconnues.
- L'**efficacité** mesurant la capacité à remplir les fonctions nécessaires pour remplir les exigences.
- La **fiabilité** spécifiant sa capacité à fournir un service auquel on peut se fier de manière justifiée. Cette propriété ne concerne pas seulement le système lui-même, mais aussi les autres acteurs et processus qui jouent un rôle au cours du cycle de vie de l'IA (ingénieurs, opérateurs, autorités de certification, compagnies d'assurance...).
- La **facilité d'utilisation** capturant la mesure dans laquelle le système peut être utilisé pour atteindre des objectifs avec efficience et satisfaction dans un contexte d'utilisation spécifique.
- La capacité des individus à interagir avec les systèmes à base d'IA, à les comprendre et à les contrôler, en veillant à ce que ces technologies soient **transparentes, explicables et alignées sur les intentions humaines** ;
- La **surveillance humaine** englobant l'évaluation et l'orientation des systèmes à base d'IA afin de s'assurer que leur fonctionnement respecte les cadres juridiques, les droits fondamentaux et la bienveillance générale.

Ces exigences prennent des formes particulières dans le cadre de systèmes critiques, notamment dans le domaine de la défense. Par exemple, la sûreté peut nécessiter une validation formelle et même une certification pour certains contextes d'application. L'auto-explication en temps réel peut être une condition nécessaire à l'acceptabilité de certains systèmes critiques basés sur l'IA et peut nécessiter un dialogue humain-machine avancé. La cybersécurité a une relation bilatérale complexe avec l'IA. Certaines caractéristiques des systèmes d'apprentissage les rendent vulnérables aux cyberattaques et au leurre même par les techniques de l'IA. À l'inverse, la capacité de certains algorithmes d'IA à identifier les irrégularités ou les anomalies peut permettre de prévenir les cyberattaques. Tous ces enjeux posent un certain nombre de défis technologiques concrets.

Pour garantir une conception algorithmique d'une IA de confiance, intégrer les paradigmes induits par l'IA ainsi que les dimensions de qualité, sûreté et (cyber)-sécurité nécessite de démontrer que les algorithmes sont corrects. Il faut alors vérifier la conformité entre leurs spécifications et leur comportement, autrement dit l'écart entre ce qu'il est supposé faire et ce qu'il fait réellement. Certaines approches en IA symbolique comme la programmation par contraintes offrent, par construction, cette propriété de correction, mais pour l'IA connexionniste par nature stochastique, cette démonstration se fait en générale via des campagnes de tests. De plus, comme la robustesse d'un système à base d'IA caractérise son aptitude à fournir des réponses correctes face à des situations inconnues ou à des malveillances, cette propriété est plus difficile à qualifier que la précision (*accuracy*). En effet, un système non précis ne peut être robuste. Mais surtout, un système précis peut ne pas être robuste. C'est le cas d'un système à base d'apprentissage ayant appris par cœur les données d'apprentissage qui se trompera dans ses décisions futures basées sur de nouvelles données. Ce phénomène

est appelé *overfitting* (sur-apprentissage). De plus, l'IA reste vulnérable, et si l'on n'y prend pas garde, particulièrement sensible aux attaques dites « *adversarial* » (antagoniste), attaques qui tirent parti du fonctionnement des algorithmes sous-jacents pour générer des perturbations de faible amplitude dans les données analysées et force l'IA à renvoyer un résultat incorrect. Heureusement, l'existence d'attaques antagoniste (*adversarial attack*) induit l'existence de défenses. De nombreuses défenses ont été proposées ces dernières années par la communauté scientifique mais elles sont parfois réfutées avec de nouvelles attaques les rendant obsolètes. Ainsi, certaines approches d'IA hybrides sont plus robustes. Citons par exemples, les PINNS (resp. les GINNs) algorithmes robustes aux bruits des capteurs, comme la vibration (resp. aux déformations géométriques comme la distorsion induite par les caméras de type *fisheyes*).

Il est aussi nécessaire de prouver que les systèmes critiques sont contrôlables, c'est-à-dire qu'ils sont bien-fondés ou cohérents (on emploie aussi l'anglicisme *consistant*), si l'on peut prouver qu'ils ne font que ce qu'on l'attend d'eux. Les questions relatives aux problèmes de robustesse et de consistance commencent à faire l'objet de travaux liés aux preuves formelles. Ces dernières visent à apporter des garanties a priori sur la sûreté de fonctionnement d'un programme, contrairement aux méthodologies de validation par expérimentations directes qui visent à apporter des garanties a posteriori. C'est pourquoi, la combinaison d'IA symbolique et connexionniste semble très prometteuse.

La fameuse « *boîte noire* » de l'IA est une préoccupation majeure pour ses développements futurs. En effet pour les systèmes critiques, il est nécessaire de comprendre pleinement comment et pourquoi l'algorithme prend une décision. Le rapport Villani « Donner un sens à l'intelligence artificielle » en souligne l'importance, déclinant ce défi en trois axes : la production de modèles plus explicables, la production d'interfaces utilisateurs plus intelligibles ainsi qu'une meilleure compréhension des mécanismes cognitifs sous-jacents. En pratique, on peut envisager de construire des systèmes hybrides qui consisteraient à mixer intelligemment IA symbolique (système à base de connaissances) aux approches à base d'apprentissage.

4.3. Intégration et embarquabilité de l'IA dans les systèmes opérationnels

L'intégration de solutions logicielles à base d'IA dans des systèmes embarqués est un sujet complexe et à la frontière entre plusieurs domaines.

4.3.1. Méthodologie de développement

Tout d'abord, l'intégration dans un système embarqué doit être prise en compte au plus tôt dans les phases de conception. Il faut en effet commencer par gérer l'écart éventuel entre l'environnement de conception et l'environnement dans lequel sera déployée la fonction. En pratique, ceci couvre deux thèmes : les données, et le matériel.

Les données utilisées pour former la base d'apprentissage de la fonction IA, ou plus généralement celles utilisées pour effectuer la conception pourraient présenter un écart avec les données rencontrées une fois le système déployé.

Aux premiers stades de la conception, il faut donc choisir la source pour constituer la base d'apprentissage, et choisir quelles données seront utilisées pour qualifier le système. Cela signifie, entre autres, déterminer la proportion de données synthétiques et de données réelles, définir le contenu des campagnes d'acquisition à effectuer, ainsi que lister les essais terrain nécessaires pour la qualification. La finalité est bien sûr le bon fonctionnement du système une fois déployé.

Sur les aspects matériels, il est important de noter que la stratégie de développement a un impact fort sur les enseignements, et arguments de qualification qui peuvent être produits. En effet, réaliser un démonstrateur à des fins de réduction de risque est une approche très différente de celle visant à réaliser un prototype de produit.

D'un point de vue plus pratique, le portage de fonctions IA sur des calculateurs embarqués implique souvent des étapes de compression, en particulier pour des applications temps-réel avec calculs complexes. L'impact fonctionnel de cette étape de compression doit être pris en compte dans le processus de développement, en particulier au moment d'effectuer la qualification du système, qui doit bien évaluer le comportement de la fonction telle qu'elle sera exécutée sur le calculateur final, dans le système déployé.

4.3.2. Adaptation aux contraintes du calcul embarqué

Le calcul embarqué est, entre autres, limité par la puissance calculatoire disponible. C'est pourquoi le recours aux modèles d'IA, souvent très calculatoires, doit être justifié. Se placer au juste besoin en termes de complexité algorithmique permet de libérer une précieuse ressource de calcul. Ceci est par exemple possible en choisissant des modèles ajustés à la tâche à assurer, ou en limitant le domaine d'emploi couvert par la fonction.

Il ne faut pas oublier que dans la majorité des cas, la fonction d'IA ne sera pas seule sur le calculateur. Le plus souvent, ces fonctions d'IA sont intégrées dans des chaines logicielles classiques assurant la cohérence d'ensemble ou d'autres fonctions, qui sont exécutées en parallèle. Ce sujet entre d'ailleurs aussi en

considération lors du choix du calculateur, qui doit pouvoir gérer les contraintes associées : cadences, latences, reproductibilité, etc.

Les ressources calculatoires disponibles en marge de la fonction d'IA peuvent également être mobilisées pour assurer un contrôle de cette fonction. Par exemple, cela peut consister à effectuer une surveillance des réponses de la fonction, ou effectuer une surveillance des entrées fournies afin de vérifier qu'elles sont bien compatibles du domaine de qualification, l'ODD (*Operational Design Domain*).

4.3.3. Problématique cyber et SSI

La sécurisation du contenu logiciel change d'échelle avec l'IA, car les volumes de données à protéger augmentent parfois en comparaison à des algorithmes traditionnels. En effet, les paramètres des modèles d'IA sont parfois très nombreux et volumineux, et doivent être protégés sous peine de révéler des indices sur le fonctionnement de la fonction ou ses performances. Cette protection nécessite parfois des compromis sur la performance d'exécution de la fonction.

4.3.4. Capacité d'actualisation de la fonction IA en contexte embarqué

Traditionnellement, la fonction d'IA est initialement entrainée avant d'être intégrée dans le système, qualifiée, et déployée. Cette vision « statique », qui représente déjà un défi industriel, est déjà en évolution avec l'émergence du besoin d'actualisation de la fonction, et donc de nouvel apprentissage.

Ce nouvel apprentissage devra être assez fréquent, et s'opérer sur le terrain de déploiement, ou tout du moins proche de celui-ci. Ce besoin mobilise, entre autres, plusieurs enjeux :

- la disponibilité des données pour affiner le fonctionnement de la fonction et garantir le bénéfice de la mise à jour ;
- l'accès à des ressources de calcul pour effectuer le complément d'apprentissage, et la mise à jour ;
- selon le contexte et les utilisateurs, une automatisation partielle ou complète du processus de mise à jour sur le terrain, de qualification, et de la vérification de non régression pour garantir le déploiement ;
- l'accès au(x) système(s) et la capacité à y charger de nouveaux paramètres.

4.4. Appropriation de l'IA par l'humain

L'emploi de l'IA dans les opérations militaires soulève d'importantes questions éthiques, particulièrement concernant l'autonomie des systèmes d'armes. Le principe fondamental du maintien de l'humain dans la boucle décisionnelle pour l'usage de la force létale demeure une préoccupation majeure. Les forces terrestres doivent élaborer des doctrines claires et des cadres juridiques adaptés pour encadrer l'utilisation de ces nouvelles technologies.

Cependant, la doctrine seule ne sera pas suffisante. Les forces et les industriels doivent travailler ensemble pour concevoir des systèmes optimisés permettant à l'opérateur de comprendre la situation afin de prendre une décision éclairée. Ces systèmes doivent inclure des éléments garantissant la confiance dans le fonctionnement et les prévisions du système, ainsi que des interfaces humain-machine (IHM) bien pensées. En effet, pour maintenir la compréhension de la situation, ces IHM devront fournir la bonne information avec le bon niveau de synthèse au bon moment. Cet adage, déjà difficile à maîtriser pour un sous-système, l'est d'autant plus dans la gestion de multiples systèmes, voire d'essaims ou de meutes.

4.4.1. Usage et facteurs humains

L'appropriation de l'IA par l'humain repose sur une alliance entre performance, traçabilité et explicabilité, éléments cruciaux pour établir une relation de confiance entre l'homme et la machine. Cette confiance est indispensable pour que l'aide apportée par l'IA soit pleinement exploitée. À l'horizon 2035, les niveaux de performance et de traçabilité semblent atteignables, mais l'explicabilité reste un enjeu majeur, notamment dans le domaine de la défense où les systèmes d'armes nécessitent des justifications claires de leurs résultats. L'intégration de l'IA dans des systèmes robotiques implique une transformation du rôle du robot, passant d'un simple outil à un véritable co-équipier. Aujourd'hui, des réticences sur l'utilisation de robots intégrant des fonctions automatisées persistent notamment en raison de la crainte de perdre la communication « H x H » (humain à humain) et de se retrouver devant des robots « incontrôlables » qui prennent des décisions de manière autonome.

4.4.2. Téléopération et Supervision

La téléopération consiste à réaliser des opérations à distance, sans la présence physique de l'opérateur au moment et/ou sur le lieu de ces opérations. Cette distinction est cruciale car elle implique une série de mécanismes humains complexes, tels que la perception délocalisée et la représentation mentale. La supervision, quant à elle, consiste à contrôler et diagnostiquer le fonctionnement d'un système, en collectant des

données permettant de fournir des indications sur son état. Les opérateurs doivent non seulement comprendre comment interagir avec des systèmes automatisés, mais aussi comment ces systèmes peuvent influencer leur perception et leur cognition. Par exemple, la perception délocalisée et la représentation mentale jouent un rôle crucial dans la manière dont les humains perçoivent et interagissent avec des environnements virtuels ou distants.

4.4.3. Charge Cognitive et Facteurs Humains

Les facteurs humains, tels que la charge cognitive, la perception, et la vigilance, sont des éléments clés dans l'appropriation de l'IA. Les opérateurs doivent être capables de comprendre et de gérer les informations fournies par les systèmes automatisés, ce qui nécessite une formation et une expérience adéquates. Les contraintes de communication et les performances nécessaires pour réaliser des tâches critiques sont également des facteurs importants à considérer. Par exemple, un conflit visuo-vestibulaire peut entraîner des effets de cinétose, une désorientation spatiale, et une perte de repère dans l'espace, ce qui peut compliquer l'appropriation de l'IA. On retrouve la même situation dans le cas d'utilisation de systèmes automatisés mobiles tels les robots terrestres ou les drones aériens, avec ou sans l'aide d'IA.

Cette évolution nécessite une organisation claire des tâches et des rôles au sein du système homme-robot, tout en tenant compte des capacités cognitives de l'opérateur. La coexistence de différents référentiels d'environnement et la capacité de l'opérateur à superviser plusieurs plateformes tout en maintenant une vision globale sont des défis cognitifs et organisationnels à relever. Pour y parvenir, il est crucial de déléguer certaines tâches au système, permettant ainsi à l'opérateur de se concentrer sur des tâches spécifiques tout en ayant la capacité de reprendre le contrôle en cas de besoin. L'implication des opérateurs dans les tâches de supervision est également essentielle, motivée par le besoin de comprendre les décisions du système, de connaître son état et de garder le contrôle. Ces mécanismes de confiance et d'acceptation technologique sont souvent renforcés par des plans de conduite au changement, facilitant ainsi l'intégration de l'IA dans les habitudes de travail.

4.4.4. Explicabilité et Confiance

L'IA doit permettre une meilleure compréhension de la situation et une plus grande réactivité dans la prise de décision. Cependant, pour que cette relation soit efficace, il est crucial que l'IA soit explicable. Les systèmes de *deep learning*, bien qu'efficaces, doivent être capables de justifier leurs décisions pour gagner la confiance des opérateurs. Les travaux en cours sur l'explicabilité de l'IA sont essentiels pour surmonter ce défi et assurer une intégration réussie de l'IA dans les systèmes militaires. Compte tenu de la gravité potentielle des effets des systèmes d'armes, les travaux visant à rendre les systèmes d'intelligence artificielle capables de fournir des justifications de leurs propres résultats doivent être vus comme un préalable à l'exploitation des technologies d'intelligence artificielle.

4.4.5. Organisationnel

L'intégration de l'IA dans les forces armées nécessite une transformation profonde de la culture militaire et des compétences requises. Les forces terrestres doivent non seulement former leurs personnels à l'utilisation de ces nouvelles technologies, mais aussi les aider à comprendre leurs limites et à maintenir un regard critique sur leurs recommandations. Ce changement culturel peut parfois représenter un défi plus important que le développement technologique lui-même.

Des travaux récents ont révélé que les opérationnels ont des attentes variées concernant l'automatisation et l'IA. Certains préfèrent une supervision directe des actions des systèmes automatisés, tandis que d'autres sont plus enclins à déléguer des tâches spécifiques à l'IA. De plus, des réticences ou des craintes subsistent, notamment liées à un manque de confiance dans la technologie proposée, ainsi qu'à des difficultés à se référer et à prendre en compte des données d'observation dans des secteurs de terrain distincts, ce qui complique la gestion des tâches de supervision et de téléopération. Ces divergences d'opinion mettent en lumière la nécessité d'une formation approfondie et d'une adaptation des processus organisationnels pour intégrer efficacement l'IA dans les opérations militaires.

En outre, des préoccupations concernant la réactivité opérationnelle existent vis-à-vis de la présence de systèmes automatisés, le cadencement important des tâches augmentant le stress perçu et la charge cognitive de l'ensemble de l'équipage. Ces préoccupations sont liées à la perception que la technologie actuelle ne permet pas de réagir aussi rapidement que les opérateurs humains lors des phases d'engagement intense.

Enfin, il reste nécessaire de disposer d'une base technique particulièrement solide pour répondre aux aléas et aux dysfonctionnements des systèmes automatisés. Cela implique une formation continue et une adaptation des compétences des opérateurs. En somme, l'intégration de l'IA dans les forces armées nécessite une approche holistique qui prend en compte non seulement les aspects technologiques, mais aussi les dimensions culturelles, organisationnelles et humaines.

4.5. Souveraineté

La souveraineté en matière d'IA désigne la capacité d'un pays ou d'une région à garder le contrôle de son infrastructure, de ses données, de sa capacité de production, de maintenance et de ses processus décisionnels liés à l'IA. Pour les fournisseurs d'IA, cela soulève plusieurs questions importantes auxquelles ils doivent répondre.

- **Localisation et stockage des données** : les gouvernements exigent de plus en plus que les données sensibles restent à l'intérieur des frontières nationales. Les entreprises d'IA doivent donc construire des centres de données locaux, mettre en place des capacités de traitement dans le pays et garantir le respect des lois sur la résidence des données. Cela peut augmenter considérablement les coûts d'infrastructure et la complexité opérationnelle.
- **Accès aux données :** les IA dirigées par les données (et en particulier à base d'apprentissage automatique) nécessitent de gros volumes de données pour être entraîné. Cependant, leur accès peut être bloqué par divers facteurs : classification, contrôle export, secrets industriels, réglementation etc. c'est pourquoi, le coût d'entrée d'un acteur sur le marché est donc dépendant de sa capacité d'accéder aux données nécessaires à l'élaboration de son produit ou service. Les environnements de simulation cherchent à contourner cette difficulté, mais le déploiement d'un système entraîné qu'à partir de données synthétiques posent plusieurs questions telles que la fiabilité. Ainsi un équilibre entre données réelles et synthétiques reste nécessaire.
- **Accès aux infrastructures pour une bonne gestion de la donnée** : en amont (pour l'entraînement) et en aval (pour l'exploitation en opération), l'accès aux infrastructures matérielles et logiciels est incontournable. Là encore les plus gros acteurs sont aujourd'hui d'origine américaine (GAFA en tête). De plus, la pile technologique logicielle couvrant la chaîne MLOps/AIOps, également de dominance américaine, est un mélange de technologie open source et propriétaires, dont les conditions d'usage peuvent changer rapidement[8].
- Des solutions de clouds alternatifs aux clouds américains existent, néanmoins si l'ensemble du tissu industriel devait rapidement s'en servir des problématiques de passage à l'échelle se poseraient.
- **Conformité réglementaire et normes** : différentes juridictions élaborent leurs propres réglementations en matière d'IA (comme la loi européenne sur l'IA, la réglementation chinoise sur l'IA ou les nouveaux cadres réglementaires américains). Les entreprises doivent s'adapter à des exigences de conformité, des normes de sécurité et des processus d'approbation variables selon les marchés, ce qui nécessite souvent des versions ou des fonctionnalités différentes pour chaque région. Les efforts des industriels dans les comités de standardisation peuvent aider à harmoniser les règles entre différentes zones.
- **Transfert de technologie et contrôle des exportations** : de nombreux pays imposent des restrictions sur les exportations de technologies d'IA, en particulier pour les modèles avancés ou ceux qui ont des applications à double usage. Les entreprises sont confrontées à des défis concernant les technologies qu'elles peuvent partager, les endroits où elles peuvent déployer certaines capacités et la manière de traiter les demandes des gouvernements concernant l'accès à la technologie ou au code source.
- **Exigences en matière de partenariats locaux** : certains gouvernements obligent les entreprises étrangères spécialisées dans l'IA à s'associer à des entreprises nationales ou à créer des filiales locales pour opérer sur leurs marchés. Cela peut impliquer le partage de la propriété intellectuelle, la formation de talents locaux ou l'abandon d'une partie du contrôle sur les opérations.
- **Exigences en matière de transparence et d'explicabilité** : les gouvernements peuvent exiger des entreprises spécialisées dans l'IA qu'elles fournissent des explications détaillées sur le fonctionnement de leurs modèles, leurs sources de données d'entraînement, les processus d'entrainement ou leurs processus décisionnels. Cela peut entrer en conflit avec les intérêts commerciaux et les avantages concurrentiels.

---

[8] Les licences open source pour YOLO varient de permissives (Apache 2.0, MIT) à restrictives (GPL-3.0, AGPL-3.0) et même à commerciales. La licence Apache 2.0 est la plus flexible pour une utilisation commerciale ou propriétaire, tandis que GPL-3.0 et AGPL-3.0 favorisent la collaboration ouverte avec des obligations de partage du code modifié :

- AGPL-3.0 (GNU Affero General Public License v3.0) : Utilisée pour YOLOv8, cette licence est stricte et impose que toute modification ou déploiement en mode SaaS ou cloud doit également être open source. Elle favorise la collaboration ouverte mais limite l'intégration dans des projets propriétaires sans partage du code modifié.
- GPL-3.0 (General Public License v3.0) : Utilisée pour YOLOv3, YOLOv5, YOLOv6 et YOLOv7, cette licence impose que toute œuvre dérivée doit également être open source sous la même licence. Elle est adaptée pour des projets collaboratifs mais peu recommandée pour des usages commerciaux propriétaires.
- Apache 2.0 : Licence permissive utilisée par YOLOX, PP-YOLO, YOLO-NAS, et d'autres. Elle permet une utilisation, modification et distribution libres, y compris dans des projets propriétaires, sans obligation de rendre le code modifié open source. Elle est idéale pour des usages commerciaux et entreprise.
- MIT License : Licence très permissive, également utilisée pour certains modèles, permettant une utilisation libre importantes.

- **Approvisionnement en hardware** : l'écosystème civil favorise le portage rapide de fonctions d'IA sur certains calculateurs embarqués. C'est en particulier le cas sur des GPU, qui permettent très facilement de réaliser des démonstrateurs embarqués. Cependant, les outils utilisés pour effectuer ce portage, comme par exemple les librairies d'optimisation ou de compression, sont souvent assez opaques et liés aux calculateurs utilisés. Ceci est une limitation de notre capacité à concevoir des algorithmes embarqués en toute maîtrise.

  Pour répondre à cela, des travaux actuellement en cours permettent l'émergence d'outils souverains comme AIDGE, porté par le CEA, et garantissant la transparence et la maîtrise dans la conception.

  Concernant le choix du calculateur lui-même, de nombreux critères entrent en considération : réglementation ITAR, coût, encombrement, consommation électrique, puissance calculatoire, tenue aux environnements, facilité d'utilisation pour le développement algorithmique et logiciel, vulnérabilité du point de vue cybersécurité, contraintes SSI (sécurité des systèmes d'information), production et approvisionnement, maintenance, évolutivité, etc.

  En effet, produire et déployer de l'IA implique des moyens techniques et notamment matériels. Aujourd'hui ces moyens sont principalement mis à disposition par des acteurs américains, eux-mêmes (encore) fortement dépendant des approvisionnements en semi-conducteurs en provenance d'Asie (Taiwan et Corée du Sud en tête). Notre industrie risque l'interdiction d'action en cas de rupture d'approvisionnement en matériel ou risque un déclassement en termes de compétitivité sur les prix si les conditions financières d'accès aux produits se dégradent (par exemple en cas de guerre commerciale). Des initiatives françaises (par exemple porté par le CEA) et européens (plan semi-conducteur de la commission européenne) tente de pallier ces faiblesses. Mais, forcé de constater qu'il n'y a pas (encore) de solutions de repli capable de passer à l'échelle à notre dépendance actuelle. Les ruptures d'approvisionnement durant le COVID ont démontré toute la faiblesse de cette dépendance sur la production industrielle (automobile en tête).
- **Choix des modèles** : afin de produire des IA de types *deep learning* des architectures de modèles sont nécessaires. Ces architectures sont en grande partie mises à disposition de manière gratuite et open-source. Néanmoins, plusieurs grands acteurs commencent à rendre payant l'accès à leur architecture (ex. Ultralytics en vision par ordinateur), voire ne les publient plus forcément (cas des entreprises produisant les grands modèles de langage). L'accès à des architectures performantes est une des conditions nécessaires pour obtenir des modèles de qualité.

  Actuellement la grande majorité des architectures sont inventées dans des entreprises ou des laboratoires américains. Là encore un resserrement de l'accès peut conduire à un retard dans les développements industriels.
- **Dépendances économiques et stratégiques** : Les pays craignent de devenir trop dépendants des fournisseurs étrangers d'IA pour leurs infrastructures critiques ou leurs prises de décision. Les entreprises d'IA doivent répondre aux préoccupations concernant la continuité des services, le contrôle des prix et les risques géopolitiques potentiels qui pourraient affecter la disponibilité des services. Ces préoccupations en matière de souveraineté obligent souvent les fournisseurs d'IA à réaliser d'importants investissements dans les infrastructures locales, à adapter leurs modèles commerciaux à différents marchés et à trouver un équilibre entre l'efficacité mondiale et les exigences d'autonomie régionale.

En essayant une synthèse, on arrive à la conclusion que la souveraineté industrielle en IA vise donc à préserver les capacités à agir (liberté d'action) des acteurs dans un secteur donné. La souveraineté d'une industrie selon cette définition pourrait donc se décliner sur plusieurs axes qui tendent à couvrir la réalité de sa chaîne de valeur ou de son processus de fabrication.

4. Quelles recommandations

4.1. Six ans après

Les contextes militaire et technologique ont radicalement évolué depuis le précédent rapport du GICAT sur l'IA pour les systèmes aéroterrestres, datant de 2020, imposant une transformation profonde des approches face à l'intégration de l'intelligence artificielle dans les systèmes de défense. À l'époque, l'objectif était déjà clair, convertir les données et les connaissances en informations exploitables. Mais la démarche restait analytique, segmentée et exhaustive, ciblant des secteurs et des cas d'usage où l'IA promettait un retour immédiat – notamment dans les domaines du commandement et contrôle (C2) et du renseignement. Pourtant, malgré les progrès, force est de constater que l'ambition initiale n'a été que partiellement atteinte, même si l'émergence de l'IA générative et multimodale offre aujourd'hui de nouvelles perspectives pour fusionner des données hétérogènes et accélérer l'adoption opérationnelle.

Cartographie TRL des briques IA — contexte défense / opérationnel certifié

Échelle TRL 1–9 (OTAN/DGA). TRL 2018 = reconversion des valeurs source (échelle 0–3 ×3 ≈ TRL indicatif) recalibrées à dire d'expert pour le contexte défense. TRL 2026 = estimation actuelle en environnement opérationnel certifié (pas usage grand public).

Brique IA	Source doc 2018 (0–3)	TRL 2018 (défense)	TRL 2026 (défense)	Évolution	Justification 2026 (contexte opérationnel certifié)
Automatique & commande	3	9	9	**stable**	Domaine mature de longue date (PID, contrôle robuste, H∞, MPC). Déployé et certifié en aéronautique (DO-178C), naval, terrestre. Les apports IA (RL, adaptive control data-driven) restent à TRL 5–6 en défense mais ne remplacent pas le socle qualifié. Pas d'évolution sur le cœur certifié.
Représentation de la connaissance	2,7	7	7	**stable**	Ontologies et graphes de connaissances restent utilisés en C2, ISR et doctrine (OTAN STANAG, modèles de menace). Renouveau via RAG et hybridation neuro-symbolique, mais pas de saut TRL en opérationnel certifié. Les approches symboliques gardent leur valeur pour la traçabilité.
Systèmes multi-agents	0	4	5	**▲ +1**	Base académique ancienne (FIPA, JADE, simulation wargaming à TRL 7+), mais le document source traite manifestement des SMA 'intelligents' décisionnels. Les agents LLM et l'essaimage drone progressent vite (essais en environnement représentatif) mais la certification et la maîtrise du comportement collectif bloquent au-dessus de TRL 5–6 en défense.
Traitement du langage naturel	2,7	7	8	**▲ +1**	NLP classique (extraction d'entités, classification OSINT) déjà à TRL 8–9 en 2018. Les LLM atteignent TRL 8 en usage non-critique (aide à la rédaction, synthèse de veille). Verrou défense : hallucinations, traçabilité, souveraineté du modèle. Usage classifié reste TRL 6–7.
Analyse et traitement d'image & vidéo	2,8	8	9	**▲ +1**	Vision par ordinateur déjà qualifiée en 2018 pour ISR (détection, tracking). Atteint TRL 9 aujourd'hui : segmentation temps réel embarquée, ATR certifié sur plateformes, drones avec détection onboard. Foundation models vision (SAM, DINO) accélèrent le cycle de qualification.
Analyse et traitement du signal & audio	2,7	8	8	**stable**	Traitement du signal radar, sonar, ELINT, COMINT = cœur de métier défense, TRL 9 historique sur les algorithmes classiques. Les apports deep learning (classification émetteurs, débruitage ASR durci) sont à TRL 7–8. Pas de saut majeur au niveau système certifié.
Fusion d'information	2,2	7	8	**▲ +1**	Fusion multi-capteurs (radar + EO/IR + ELINT) déjà mature en 2018. Progression forte via fusion multimodale apprise (texte + image + signal) pour ISR et renseignement. Encore des verrous sur la quantification d'incertitude en environnement contesté/dégradé.
Optimisation, planification & RO	2,3	7	8	**▲ +1**	PLNE, heuristiques, solveurs matures pour logistique, mission planning, allocation de ressources. Hybridation avec RL et ML pour la planification dynamique en cours d'industrialisation. Solveurs quantiques encore TRL 3–4. Progression nette en contexte C2 et soutien.
Raisonnement à base de connaissances & règles	2,1	7	7	**stable**	Systèmes experts et moteurs de règles restent indispensables en défense pour la traçabilité, l'auditabilité et la certification (ROE, aide à la décision). Stable en TRL mais perte de centralité face aux approches apprises. Valeur stratégique maintenue pour le certifiable.
Analyse de données et statistiques	1,7	5	8	**▲▲ +3**	Saut majeur grâce à l'industrialisation data (plateformes souveraines type Palantir, stacks MLOps durcies, BI augmentée). Passage d'un usage artisanal à des chaînes outillées et déployées en opérationnel pour la veille, le MCO prédictif, le renseignement.
Apprentissage machine (dont deep learning)	1,5	5	8	**▲▲ +3**	Révolution structurante depuis 2018. Deep learning passe de POC à déploiement opérationnel : vision embarquée qualifiée, modèles de langage souverains (Mistral, Llama on-premise), MLOps durcie. Le TRL 9 n'est pas atteint en défense à cause des enjeux explicabilité et certification.
Méthodes évolutionnaires	1	4	5	**▲ +1**	Algorithmes génétiques, CMA-ES utilisés ponctuellement pour optimisation non convexe (design antenne, trajectoires). Reste un outil niche, largement concurrencé par le deep RL. Progression modeste, usage expert et ciblé.
Théorie des jeux	1	4	6	**▲ +2**	Montée via le multi-agent RL, le wargaming assisté IA, la cyberdéfense (jeux de poursuite). Intégrée dans les outils d'aide à la décision stratégique et la simulation. Reste majoritairement en environnement de simulation/démonstrateur, peu en opérationnel direct.

Entre-temps, la France s'est dotée de l'**AMIAD** (Agence militaire d'intelligence artificielle de défense), marquant une volonté de structurer cette transition. Mais le vrai changement de paradigme réside dans le passage d'une logique analytique à une approche holistique et systémique. Il ne s'agit plus seulement d'identifier des niches technologiques, mais de repenser l'IA comme un écosystème intégré, où l'automatisation, la délégation à la machine et la résilience des systèmes deviennent des enjeux centraux. Les leçons du théâtre ukrainien ont confirmé cette nécessité : l'innovation militaire est désormais tirée par des acteurs civils, souvent plus agiles, tandis que les armées doivent composer avec des cycles de développement accélérés et une compétition technologique sans précédent.

Les points de vigilance identifiés il y a six ans restent cruciaux : souveraineté des données et des infrastructures, volume et qualité des corpus d'apprentissage, hybridation des techniques d'IA, et adaptation aux environnements dégradés. Pourtant, l'avance du civil s'est creusée, et la guerre en Ukraine a révélé à quel point des acteurs non étatiques ou privés peuvent bousculer les équilibres stratégiques en transposant rapidement des innovations duales. Ces six années ont démontré une réalité : sans une volonté politique forte et une coordination systémique, la France ne pourra pas rivaliser avec des compétiteurs qui, eux, intègrent l'IA à un rythme soutenu et sans les contraintes éthiques ou réglementaires qui pèsent sur les démocraties. L'enjeu n'est plus seulement technologique, mais stratégique et organisationnel : passer d'une logique de silos à une vision globale, où l'IA devient un multiplicateur de capacités – et non un simple outil.

4.2. Les grands défis d'aujourd'hui

4.2.1. Donnée et connaissance : le duo gagnant

Dans le contexte exigeant des opérations militaires des forces terrestres, l'IA hybride, combinant les approches dirigées par les données avec celles à base de connaissances, se révèle particulièrement pertinente pour répondre aux défis spécifiques liés à la disponibilité des données, à la robustesse des systèmes et à l'intégration de la connaissance métier. En effet, il est souvent difficile d'obtenir des données fraîches, complètes et représentatives – notamment pour des tâches comme la classification ou la détection automatique de menaces – en raison de leur nature sensible ou parfois indisponible en temps réel. Il devient alors essentiel de pouvoir exploiter des données "d'opportunité" : données anciennes, issues d'exercices, moins sensibles mais néanmoins précieuses. Cependant, travailler uniquement avec des données ne suffit pas : la connaissance métier, c'est-à-dire l'expertise opérationnelle, tactique et stratégique propre aux forces, confère un avantage décisionnel unique, difficilement reproductible par d'autres acteurs.

Pour maximiser les bénéfices de l'IA, il est aussi crucial d'intégrer cette connaissance métier dès les premières phases de conception des systèmes, en parallèle avec le développement des technologies (IA, capteurs, etc.) afin que les modèles soient « orientés » par les besoins et contraintes opérationnels. Cela permet de concevoir des systèmes à la fois plus efficaces, mieux adaptés au contexte terrain et plus explicables.

Sur le plan technique, les approches classiques d'IA présentent encore des limites notables. Les méthodes statistiques et connexionnistes – basées sur de grandes quantités d'exemples – manquent souvent de transparence et d'interprétabilité, ce qui réduit la confiance des utilisateurs opérationnels. Elles sont également peu robustes face à des situations inédites ou adverses, et consomment beaucoup de données et d'énergie, ressources parfois rares en contexte déployé. À l'inverse, l'IA symbolique, qui utilise des règles explicites et du raisonnement formel, apporte une meilleure explicabilité, mais sa robustesse face aux incertitudes ou aux situations non modélisées reste limitée. Combiner les forces des approches connexionnistes (réseaux de neurones, apprentissage profond) et symboliques, et intégrer les connaissances métier, physiques et mathématiques disponibles permet d'accroître l'interprétabilité des modèles, leur robustesse opérationnelle et facilite leur validation en vue d'homologations nécessaires sur les systèmes critiques militaires.

Les programmes de recherche tels que le ANSR (*Assured Neuro Symbolic Learning and Reasoning*), lancé par la DARPA en 2022, incarnent cette démarche en développant des algorithmes intégrant intimement raisonnement symbolique et apprentissage automatique, pour aboutir à des systèmes fiables, sûrs et dignes de confiance.

Parmi les innovations les plus prometteuses, les *Physics-Informed Neural Networks* (PINNs) apportent une hybridation entre réseaux neuronaux et modèles physiques. En contraignant l'apprentissage à respecter les lois fondamentales de la physique modélisées via des équations différentielles, les PINNs réduisent l'espace des solutions possibles, augmentant la fiabilité et l'explicabilité des résultats. Cette technologie, applicable par exemple à la mécanique des fluides, l'électromagnétisme ou la thermique, ouvre d'importantes perspectives dans la défense, notamment à travers les jumeaux numériques, qui permettent de simuler en temps réel et avec une grande précision les comportements complexes des équipements et environnements opérationnels. Par ailleurs, l'approche des *Geometric-Informed Neural Networks* (GINNs) utilise la géométrie de l'information pour mieux appréhender la structure des espaces de paramètres des réseaux multicouches. Cette technique a déjà permis des preuves de concept dans des applications militaires critiques telles que la détection et reconnaissance automatique de cibles (ATDR) à partir de signatures micro-Doppler, l'analyse fine des trajectoires cinématiques ou encore la reconnaissance visuelle à partir de caméras 360° *fisheye*.

L’exploitation intelligente des données conjuguée à la valorisation de la connaissance métier et l’intégration rigoureuse des lois physiques et mathématiques, permet de construire des systèmes d’IA adaptés aux exigences de robustesse, d’interprétabilité et de confiance indispensables aux forces terrestres. Cette approche ouvre la voie à des capacités accrues sur le champ de bataille, en renforçant la prise de décision, la détection précoce des menaces et la gestion efficace des ressources dans un environnement toujours plus complexe et incertain.

4.2.2. Vulnérabilités cybernétiques

La dépendance accrue envers les systèmes intelligents crée de nouvelles vulnérabilités face aux cyberattaques. Un adversaire capable de compromettre ou de perturber les algorithmes d'IA pourrait neutraliser l'avantage technologique ou, pire encore, retourner ces systèmes contre leurs utilisateurs. Les forces terrestres doivent donc développer des protocoles de cybersécurité robustes et des capacités de fonctionnement en mode dégradé.

Parmi les menaces les plus importantes, on trouve les attaques visant à modifier le fonctionnement du modèle. La sécurisation de l'apprentissage de l'IA sur des données sensibles contre les fuites d'informations et la protection des droits d'auteur dans un contexte complexe sont également des préoccupations majeures. En attendant les réglementations, les professionnels cherchent des contremesures pour allier protection et performance.

Pour assurer la traçabilité d'un modèle partagé, le créateur peut utiliser des techniques de tatouage, inspirées des solutions de marquage pour les supports multimédias. Le tatouage de modèle d'IA vise à protéger la propriété intellectuelle en intégrant une preuve d'origine dans l'architecture ou le comportement du modèle. Les techniques de tatouage se divisent en deux catégories principales : « boîte blanche » et « boîte noire ». En boîte blanche, la preuve de propriété repose sur une modification secrète intégrée dans les paramètres ou l'architecture du modèle. En boîte noire, elle prend la forme d'une modification secrète intégrée dans le comportement du modèle.

L'apprentissage fédéré permet l'entraînement de modèles directement sur des dispositifs locaux, les mises à jour étant agrégées en un modèle global sans que les données brutes ne quittent chaque dispositif. Cela facilite la collaboration et réduit les risques de sécurité des données. Cependant, l'apprentissage fédéré ne protège pas le modèle final des fuites d'information, surtout si un attaquant s'introduit dans le serveur d'agrégation. Pour se prémunir contre cela, des techniques de chiffrement homomorphe et de confidentialité différentielle peuvent être utilisées.

Une stratégie de sécurité efficace commence par l'identification des actifs à protéger, tels que les données d'entraînement, le modèle ou les données d'entrée/sortie. Elle se poursuit par une étude des menaces potentielles et de leurs impacts en fonction des capacités de l'attaquant. Dans un scénario « boîte-blanche », l'attaquant a accès à tout le modèle, tandis qu'en « boîte-noire », il ne peut que l'interroger. Des mesures correctives peuvent ensuite être mises en œuvre pour améliorer la robustesse du modèle ou ajouter des défenses dans le système.

L'empoisonnement des données est une autre menace majeure. Un attaquant ayant accès à la chaîne d'approvisionnement des données d'un modèle peut chercher à la manipuler pour empoisonner le modèle, dégradant ainsi ses performances. L'empoisonnement peut également servir à insérer des fonctionnalités inconnues de l'utilisateur légitime, appelées portes dérobées. Un exemple notable est le chatbot TAY de Microsoft, qui a dû être mis hors service après que des internautes malveillants lui aient fait tenir des propos haineux.

L'IA générative pose également des défis spécifiques. Les grands modèles linguistiques (LLM) sont la nouvelle cible des pirates informatiques. L'injection de *prompts* permet aux pirates d'utiliser des entrées soigneusement conçues pour manipuler le LLM afin qu'il exécute des instructions potentiellement malveillantes. Cela peut conduire à la manipulation des réponses du modèle ou de tout processus décisionnel qu'il influence ou contrôle. Les attaques de *jailbreaking* consistent à demander à l'IA d'adopter une identité différente pour discuter d'actes illégaux, de contenus haineux ou de désinformation. Les *deepfakes*, générés par des *chatbots*, peuvent être utilisés pour tromper les systèmes biométriques, pour des attaques d'ingénierie sociale ou pour la guerre de l'information.

4.2.3. Interopérabilité et standardisation

L'action de déployer une IA ne se résume pas seulement au fait d'installer et d'exécuter un code informatique en isolation. Les IA seront déployées au sein de systèmes qui intègrent des senseurs, des effecteurs, des utilisateurs, des liaisons de données et des composants non-IA, tous en interaction. L'architecture de ces systèmes doit donc prendre en compte la manière dont ces composants doivent interagir entre eux. Afin de favoriser l'interopérabilité, il est possible de distinguer plusieurs étapes dans le cycle de vie des systèmes IA où ceux-ci doivent être en mesure d'avoir des interfaces, ou a minima des descriptions, standardisées :

- en conception : sur les types et formats de données utilisées par chaque composant, le domaine d'emploi prévu du système, ainsi que les méthodes utilisées pour le concevoir (e.g., type d'entrainement dans le cas de l'apprentissage) ;
- en validation : sur les performances atteintes et les limitations connues du système ;
- en intégration : sur les contraintes en termes de matériels pour garantir les performances ;
- en production : sur les formats des flux de données produits et les alertes éventuels à l'usage ;
- en maintenance : sur les formats de données captées et le domaine d'emploi correspondant, sur les performances atteintes et les incidents détectés.

La standardisation de ces formats, interfaces et descriptions permet une utilisation facilitée par les acteurs de la chaîne de valeur (opérateurs, intégrateurs, maintenanciers, fournisseurs, déployeurs). À ce jour les systèmes d'IA sont parfois conçus en isolation du reste du système et leur description reste souvent dépendante du fournisseur (souvent venant du monde civil) qui peut définir encore lui-même ses propres formats de description. Dans certains cas les informations fournies ne permettent pas forcément d'apprécier le cadre d'usage ou les performances du système en ne fournissant qu'une partie des métriques nécessaires. Des efforts de standardisation sont en cours dans le monde civil (e.g., au CEN-CENELEC JTC 21, à l'ISO/IEC JTC 1/SC 42) et de tels documents pourront servir de base pour une déclinaison militaire de standards dans un cadre comme celui de l'OTAN ou de l'EDA.

Dans un contexte d'opérations interarmées et multinationales, l'interopérabilité des systèmes d'IA constitue un enjeu crucial. L'harmonisation des formats de données, des protocoles de communication et des interfaces homme-machine est nécessaire pour garantir l'efficacité opérationnelle des forces coalisées.

4.2.4. IA explicable

Les systèmes d'IA sont souvent décrits comme des boites noires dont il est difficile d'extraire des justifications de ce qu'elles produisent. Ce constat est globalement vrai pour les IA du monde de l'apprentissage machine et particulièrement vrai dans le cas de l'apprentissage profond. Néanmoins certaines techniques plus symboliques portent en elle une capacité à justifier leur production.

Pour un utilisateur la confiance dans un système se construit en partie au travers une relation avec le système où il peut comprendre et anticiper ses actions. L'ISO/IEC distingue deux niveaux liés à cette compréhension : l'explicabilité et l'interprétabilité[9]. Dans le cas de l'interprétabilité le système fournit des informations de bas niveau pour analyser ce qui dans les entrées du système contribue à produire ses sorties. Ce niveau est en général utilisé par les concepteurs du système pour vérifier son comportement et y apporter des corrections le cas échéant (y compris pour l'apprentissage automatique, dont en particulier l'apprentissage profond). Dans le cas de l'explicabilité le système peut fournir une analyse compréhensible (donc proche du niveau d'un raisonnement humain et possiblement en langage naturel) par un utilisateur qui n'est pas un expert de l'IA ni un concepteur du système.

Pour renforcer la confiance des opérateurs et maintenir un contrôle humain significatif, les futurs systèmes d'IA militaires devront être capables d'expliquer leur raisonnement et leurs recommandations de manière claire et compréhensible. Pour cela il est nécessaire de mesurer les attentes des utilisateurs, mais également le niveau de formation de ces utilisateurs. En effet l'explicabilité doit être adapté au niveau de compréhension que peut avoir l'utilisateur et du temps nécessaire à cet utilisateur pour l'analyser.

4.2.5. Repenser l'ingénierie des systèmes à base d'IA

De nombreux verrous freinent encore l'adoption de l'IA, en particulier pour un déploiement dans les systèmes critiques. Ceux-ci doivent par construction garantir des propriétés de fiabilité, de maintenabilité, de disponibilité de sûreté et de sécurité (RAMS: *Reliability, Availability, Maintainability, Safety*), mais aussi suivre des principes d'éthique et de responsabilité des opérations terrestres, il est indispensable de revisiter profondément les différentes ingénieries comme l'ingénierie algorithmique, logicielle, système mais aussi l'ingénierie de la donnée, l'ingénierie des connaissances sans oublier l'ingénierie de la cybersécurité, de la sûreté (*safety*) et l'ingénierie cognitive. En effet, l'intégration de l'IA y adopte une démarche souvent proche de l'expérimentation, nécessitant de repenser nos méthodes de travail traditionnelles. Il ne suffit donc plus de valider une solution ponctuelle, mais il faut privilégier une intégration et une qualification incrémentales, permettant d'adapter progressivement les systèmes tout en garantissant leur robustesse.

[9] Dans le standard ISO (ISO/IEC 22989 :2022 – AI: Overview of trustworthiness concepts), l'explicabilité est définit comme la capacité d'un système d'IA à fournir, de façon compréhensible pour l'humain, des informations sur le fonctionnement interne qui permettent de justifier une décision ou un comportement alors que l'interprétabilité représente le degré auquel un être humain peut saisir les relations de cause à effet entre les entrées, les processus internes et les sorties d'un système d'IA, afin de comprendre pourquoi une décision a été prise.

De plus, l'IA est par nature très contextuelle, ce qui impose une capacité d'adaptation aux évolutions et changements de contexte opérationnels. Cela implique un dialogue permanent entre utilisateurs opérationnels, les ingénieurs systèmes et les développeurs comme les « *data scientists* », afin d'identifier les données/connaissances réellement pertinentes – par exemple issues d'exercices – et de systématiser leur extraction, leur collecte, leur qualification et leur exploitation. En particulier, les équipements et systèmes doivent être outillés pour cette collecte et cet usage efficace des données.

Dans le cadre plus spécifique de la défense, un enjeu majeur consiste à éviter la rétro-ingénierie en cas de compromission du système par un ennemi. Cela conditionne fortement les choix architecturaux et de sécurité autour de l'IA embarquée.

Enfin, si la preuve de concept d'une application IA est souvent facile à obtenir, passer à une solution industrielle fiable et adaptée aux contraintes militaires s'avère complexe. L'ingénierie de l'IA doit alors intégrer non seulement la montée en charge, mais aussi la maintenance continue, les mises à jour régulières et la garantie de performance dans la durée. Cette transformation globale des processus d'ingénierie est un prérequis incontournable pour exploiter pleinement le potentiel de l'IA dans les systèmes critiques y compris pour les opérations terrestres.

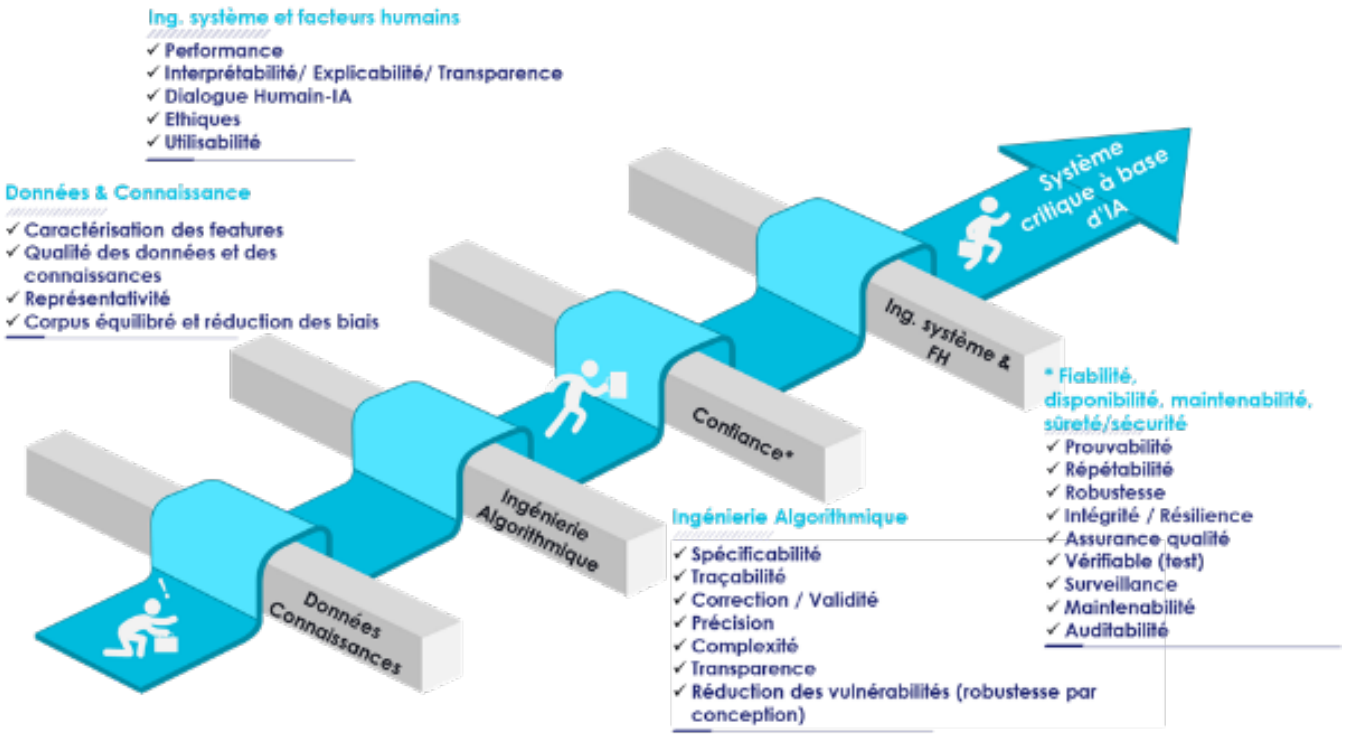


Figure 15 : L'introduction de l'IA induit de nouveaux enjeux d'ingénierie (©Thales 2024)

Ainsi pour déployer de l'IA dans des systèmes critiques, notamment dans le domaine

Ainsi, le développement d'un système à base d'IA doit reposer sur des méthodes de développement bien fondées, de sa conception à son déploiement et sa qualification, ce qui induit de nouveaux enjeux d'ingénierie (voir Figure 15).

Les pratiques d'ingénierie doivent être alors revisitées et enrichies par des méthodes et outils garantissant la confiance à toutes les étapes du cycle de vie d'un tel système : (1) l'analyse du domaine opérationnel (OD : Operational Domain) au regard de l' « *intended purpose* » ; (2) spécification du domaine opérationnel (ODD: *Operational Design Domain*) et sa déclinaison pour la gestion des données et des connaissances ; (3) conception d'algorithmes et d'architecture; (4) caractérisation, vérification et validation ; (5) déploiement, en particulier sur une architecture embarquée ; (6) qualification, certification et (7) maintien en condition opérationnelle et de cybersécurité.

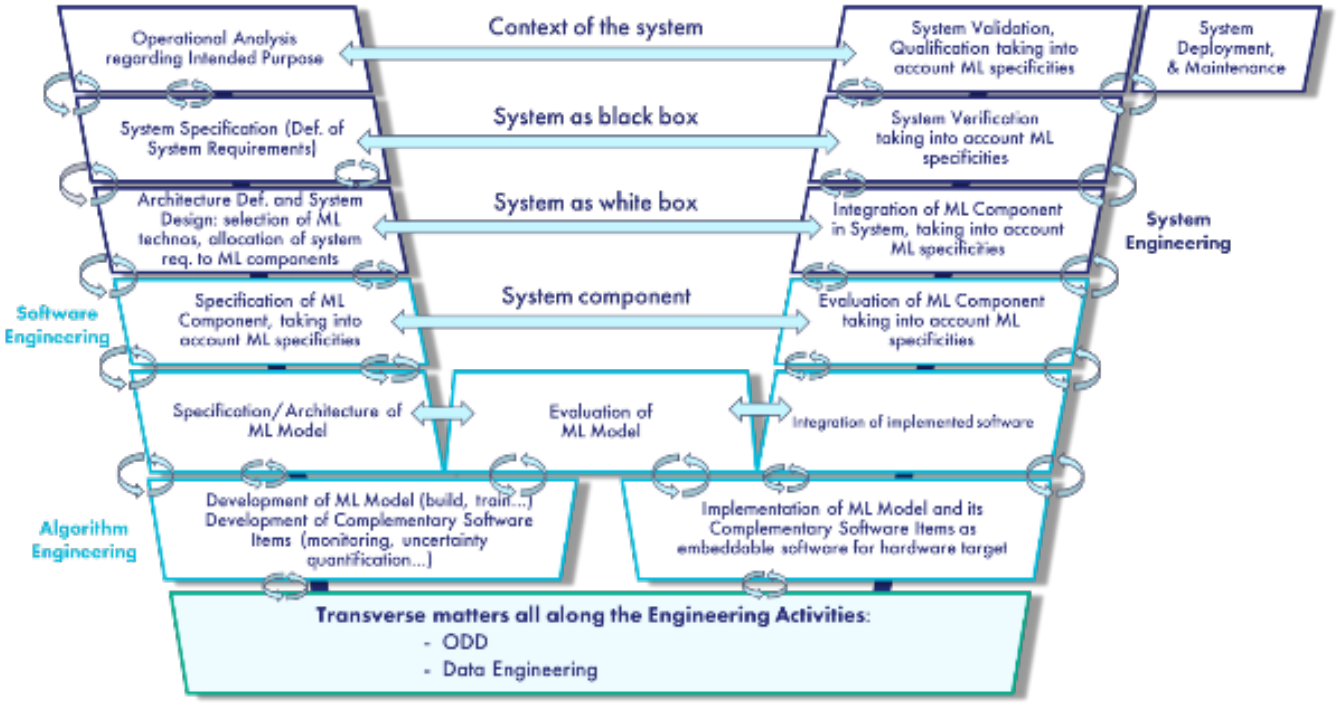


Figure 16 : Référentiel de l'ingénierie de l'IA responsable et industrielle, définie dans le "Body of Knowledge" du programme Confiance.ai et intégrant la méthodologie de bout-en-bout

Pour répondre à ce défi, la France a lancé de nombreuses initiatives, comme le cluster IA ANITI[10] avec son projet DEEL[11] et le programme Confiance.ai[12] qui ont permis de définir des méthodologies et des outils d'une ingénierie de l'IA industrielle et responsable, transforme le classique cycle de vie en « V » d'un système en « W »[13] et couvrant les étapes suivantes.

– **La spécification du problème**, capturée au travers de l'analyse du domaine opérationnel (OD : *Operational Domain*) ainsi que l'*intended purpose* désignant l'ensemble des fonctions, tâches et objectifs pour lesquels le système d'IA va être conçu. Cette étape inclut la définition des exigences de performance, les contraintes d'utilisation et les limites d'application prévues par le fabricant ou le développeur, des différentes exigences (fonctionnelles/non fonctionnelles) et de la couverture opérationnelle, description des conditions dans lesquelles la capacité est conçue pour fonctionner correctement comme les conditions environnementales et d'autres contraintes du domaine. Ceci impacte la tâche de collecte des données et de modélisation des connaissances mais aussi la définition claire des ConOps (*Concepts Opérationnels*) puis de l'ODD[14] qui précise ainsi le contexte opérationnel dans lequel le système d'IA peut fonctionner en toute sécurité et

[10] ANITI (2024). Artificial and Natural Intelligence Toulouse Institute. https://aniti.univ-toulouse.fr/

[11] DEEL (2024). DEEL PROJECT. Dependable, Certifiable and Explainable Artificial Intelligence for Critical Systems. https://www.deel.ai

[12] Confiance ai (2024). The community to accelerate the deployment of responsible AI un industrial systems. https://www.confiance.ai/

[13] EASA (2021). Concept Paper: First usable guidance for Level 1 machine learning applications. European Union Aviation Safety Agency

[14] Rappelons que :

– Intended Purpose : désigne l'ensemble des fonctions, tâches et objectifs pour lesquels le système d'IA a été conçu, incluant les exigences de performance, les contraintes d'utilisation et les limites d'application prévues par le fabricant ou le développeur.

– Operational Design Domain (ODD) : définit les conditions d'exploitation spécifiques dans lesquelles un système d'IA est censé fonctionner en toute sécurité.

– Concept of Operations (ConOps) incluant Operational Domain (OD) : décrit les scénarios d'exploitation du point de vue de l'utilisateur, les procédures et l'environnement.

– Le ConOps (incluant l'OD) et l'ODD sont interdépendants : le ConOps fournit les exigences opérationnelles, tandis que l'ODD traduit ces exigences en un espace de paramètres multi-dimensionnel qui doit être couvert par les activités de validation. En résumé, le intended purpose fixe « le quoi », i.e., ce que le système doit faire, tandis que l'ODD définit « le où », dans quelles conditions et « le comment », i.e., ce que le système peut le faire en respectant les exigences de sécurité et de performance.

conformément à son *intended purpose*. Ainsi l'ODD décrit les paramètres environnementaux, les scénarios d'usage et les restrictions techniques.

- **L'acquisition des données/connaissances** guidée par l'ODD aboutit à une agrégation des données/des connaissances en un ensemble homogène, de taille et de qualité (compréhensibles, pertinentes, fiables, équilibrées...) suffisante. Cependant, pour pouvoir être utilisées, celles-ci sont en général nettoyées, organisées, voire labellisées. Dans certains cas, un traitement est nécessaire afin de rendre ces informations brutes exploitables. Il s'agit de la tâche de « *data engineering* » (ingénierie des données) pouvant être complétée par du « *knowledge engineering* » (ingénierie des connaissances).
- **L'aide à la conception/paramétrisation** d'un algorithme d'apprentissage : même si un algorithme statistique ou connexionniste peut être conçu ou sélectionné dans une bibliothèque d'algorithmes, une fois l'apprentissage terminé, le modèle est affiné en utilisant l'ensemble des données de validation. Cela peut impliquer la modification ou l'élimination de variables, l'ajustement des paramètres spécifiques du modèle (hyperparamètres) jusqu'à un niveau de précision acceptable. L'implémentation sur la plate-forme matérielle et/ou le système cible peut impacter certaines exigences techniques comme la latence, l'espace mémoire ou la consommation énergétique.
- Après avoir trouvé un ensemble acceptable d'hyperparamètres et optimisé la précision du modèle, ce dernier est testé et caractérisé sur un ensemble de données, voire évalué par une vérification formelle. **L'évaluation** peut aller au-delà de la performance fonctionnelle (telle que la précision) et englober des métriques relatives à tout autre critère de performance attendu comme la robustesse aux bruits et/ou aux attaques adverses.
- Enfin, il faut démontrer que l'**intégration** d'une composant ML/IA conserve les « propriétés de confiance attendues. Il faut donc définir un cadre d'analyse d'« Ingénierie système de l'IA de confiance » permettant d'élaborer les stratégies de développement de systèmes et d'IVVQ (Intégration, Vérification, Validation, Qualification).

4.3. Conclusions

L'intelligence artificielle représente un multiplicateur de forces considérable pour les armées de terre modernes. En augmentant les capacités d'analyse, de décision et d'action, tout en réduisant l'exposition des soldats aux risques, elle transforme profondément la conduite des opérations terrestres. En effet, l'évolution rapide des technologies d'IA laisse entrevoir de nouvelles applications prometteuses pour les forces terrestres.

- **Systèmes multi-domaines intégrés** : L'avenir réside dans l'intégration parfaite des capacités terrestres, aériennes, navales, spatiales et cyber au sein de systèmes de combat multi-domaines. L'IA jouera un rôle central dans cette coordination complexe, permettant une synchronisation précise des effets militaires à travers les différents milieux.
- **Essaims de robots collaboratifs** : Les progrès en matière d'IA distribuée et d'apprentissage collaboratif permettront le déploiement d'essaims de robots terrestres capables d'opérer de manière coordonnée pour des missions de reconnaissance, de sécurisation de zone ou d'appui feu.

Toutefois, cette révolution technologique ne se fera pas sans défis.

L'avantage stratégique appartiendra aux nations qui sauront non seulement développer ces technologies de pointe, mais aussi les intégrer judicieusement dans leurs doctrines d'emploi et leurs structures organisationnelles, tout en formant adéquatement leur personnel à leur utilisation optimale. Dans cette course à l'innovation, l'équilibre entre avancée technologique et sagesse dans l'emploi de ces nouveaux outils sera la clé du succès.

La souveraineté stratégique de la France en matière de défense et d'IA ne peut plus se contenter d'une approche passive ou fragmentée. Face à un contexte géopolitique et militaire en profonde mutation – marqué par l'émergence de menaces densifiées, accélérées et asymétriques, l'effacement des frontières entre civil et militaire, et la montée en puissance d'acteurs étatiques ou non étatiques moins contraints par les normes éthiques ou juridiques – la France doit renforcer son autonomie décisionnelle et opérationnelle. Pourtant, cette autonomie ne signifie pas un repli sur soi ou une logique du « tout faire soi-même ». Elle exige plutôt une stratégie équilibrée, combinant maîtrise des technologies critiques comme l'IA, coopérations ciblées avec des partenaires de confiance, et agilité industrielle pour s'adapter aux ruptures technologiques.

L'enjeu est double : d'une part, **réduire les dépendances externes** dans des domaines clés – qu'il s'agisse des capacités conventionnelles (stocks, production réversible, drones low-cost), de l'intelligence artificielle souveraine (données, infrastructures, modèles), ou des systèmes autonomes (attribution, résilience, interopérabilité) ; d'autre part, **accélérer l'innovation** en acceptant de lever temporairement certaines contraintes qui freinent l'expérimentation. Aujourd'hui, les délais juridiques, éthiques ou administratifs ralentissent la validation opérationnelle et la qualification incrémentale des solutions, alors même que des adversaires ou concurrents testent, déploient et améliorent leurs systèmes en conditions réelles – comme le montre le conflit ukrainien. Pour combler ce retard, il est impératif de créer des cadres d'expérimentation plus souples, permettant aux industriels et aux forces terrestres de :

- valider rapidement des concepts (drones imprimés en 3D, IA embarquée, systèmes consommables) dans des environnements contrôlés mais réalistes ;
- **itérer sur des prototypes sans attendre une certification complète**, en adoptant une approche par étapes (qualification progressive) ;
- anticiper les usages duaux en collaborant avec des acteurs civils innovants, tout en maximisant la souveraineté des technologies sensibles.

La création de l'AMIAD et les initiatives comme celles de Thales avec cortAIx ou de Safran avec SafranAI montrent que la France a bien pris conscience du problème voire des solutions.

Mais pour passer de l'analyse à l'action, il faut oser une approche systémique : fédérer les écosystèmes (recherche, industrie, opérationnels), simplifier les processus pour les projets critiques, et accepter un niveau de risque calculé dans l'expérimentation – sans pour autant renoncer aux garde-fous essentiels en matière de sécurité et d'éthique. La souveraineté ne se décrète pas ; elle se construit par l'action, en apprenant plus vite que l'adversaire, tout en préservant les alliances stratégiques qui renforcent notre résilience collective. Le temps de la réflexion pure est révolu : place à l'itération rapide et à la validation terrain.

Cependant, la dépendance aux technologies et normes américaines – qu'il s'agisse de *frameworks* logiciels (Kubernetes, Docker), d'infrastructures cloud (AWS, Microsoft Azure), de puces spécialisées (NVIDIA), de technique et méthodologique comme le MOSA[15] (Modular Open System Architecture) ou de plateformes d'IA (Dataiku, Palantir) – constitue un risque stratégique majeur pour la souveraineté européenne et française. Ces outils, souvent soumis à des régulations extraterritoriales comme l'ITAR (International Traffic in Arms Regulations) ou l'EAR (Export Administration Regulations), peuvent à tout moment devenir des leviers de pression géopolitique : restriction d'accès, blocage des mises à jour, ou pire, exfiltration de données sensibles sous couvert de conformité légale.

Pour la France et l'Europe, l'urgence n'est pas seulement de développer des alternatives souveraines (comme les projets de cloud de confiance, les accélérateurs IA européens, ou les *frameworks open-source* contrôlés), mais aussi de repenser les standards eux-mêmes. Aujourd'hui, les normes techniques (ISO, IEEE) et les cadres d'interopérabilité (OTAN, UE) sont largement influencés – voire dominés – par des acteurs américains et chinois, ce qui perpétue une asymétrie stratégique. Pour briser ce monopole, la France et ses partenaires européens doivent :

- **Investir massivement dans les organismes normatifs** (ISO, IEC, CEN-CENELEC, ETSI) pour proposer des standards alternatifs, notamment dans :
- l'IA de défense (modèles d'apprentissage fédéré, auditabilité des algorithmes) ;
- les infrastructures cloud souveraines (interopérabilité sans dépendance à AWS/Azure) ;
- les architectures logicielles critiques (alternatives à Kubernetes ou Docker, comme K3s ou OpenShift sous contrôle européen).
- **Promouvoir des coalitions industrielles européennes** pour certifier des solutions "ITAR-free", en s'appuyant sur :
- des alliances comme l'European Defence Fund ou le Permanent Structured Cooperation (PESCO) ;
- des partenariats public-privé pour développer des chaînes d'approvisionnement résilientes (ex : puces RISC-V, *frameworks* IA open-source comme Hugging Face).

De plus, le développement d'une nouvelle discipline dédiée à l'**ingénierie de l'IA de confiance** apparaît comme une nécessité stratégique pour la France, afin de relever les défis technologiques, économiques et géopolitiques de demain, en particulier pour déployer des solutions à base d'IA de confiance au service des opérations terrestres. En effet, bien que l'IA générative et agentique dominent actuellement les investissements, d'autres sous-disciplines, comme l'IA symbolique, hybride ou distribuée sont pertinentes pour déployer des capacités innovantes pour les forces terrestres et essentielles pour garantir des propriétés critiques : fiabilité, robustesse, transparence et maintenabilité. Ces qualités sont indispensables non seulement pour instaurer la confiance dans les systèmes d'IA, mais aussi pour qualifier ou homologuer ces systèmes dans un contexte où la souveraineté technologique et la résilience face aux cybermenaces deviennent des enjeux majeurs. Par ailleurs, comme mentionné ci-dessus, l'écosystème français souffre aujourd'hui d'un manque de standards harmonisés, d'outils convergents dans la chaîne de valeur de l'IA, et d'une dépendance aux géants du numérique. Une ingénierie dédiée permettrait de fédérer les acteurs (industriels, académies, startups) autour de méthodes communes, d'accélérer le développement de solutions souveraines et frugales, et de renforcer la cybersécurité des systèmes – un impératif face à l'émergence de menaces comme les *deepfakes* ou les attaques sur les données sensibles. Enfin, cette nouvelle discipline qu'est l'ingénierie de l'IA de confiance, est un véritable levier pour anticiper les ruptures technologiques (QuantumAI) et pour positionner la France comme un leader européen en IA de

[15] Initiée par le U.S. Department of Defense (DoD) dans les années 1990, puis adoptée par de nombreux gouvernements et organisations internationales, le MOSA est une méthodologie d'ingénierie visant à concevoir des systèmes composés de modules interchangeables, favorisant la réutilisation, l'interopérabilité et la mise à jour évolutive.

confiance, en alignement avec les réglementations et les initiatives comme l'« *European Trusworthy AI Association*[16] » ou les *data spaces* souverains.

Enfin, l'**attractivité** des talents représente aujourd'hui un enjeu stratégique majeur pour les organisations, notamment dans des secteurs innovants comme celui de la défense et des technologies critiques. Attirer des profils compétents, diversifiés et motivés permet non seulement de renforcer la performance et l'agilité des équipes, mais aussi d'anticiper les défis mentionnés précédemment. Cependant, cette attractivité ne suffit pas à elle seule : elle doit s'accompagner d'un investissement continu dans la **formation** et l'**acculturatio**n à l'IA pour l'ensemble des forces terrestres et des parties prenantes. En effet, l'IA, en pleine expansion, transforme aussi les métiers, les processus décisionnels et les modes de collaboration. Pour en tirer pleinement parti, il est indispensable de démocratiser son usage, d'en maîtriser les outils et d'en comprendre les enjeux éthiques et opérationnels. Une telle démarche garantit non seulement l'adaptation des équipes aux évolutions technologiques, mais aussi la pérennité de l'avantage compétitif et la résilience des organisations face aux mutations du paysage industriel et sécuritaire. En combinant attractivité des talents et montée en compétences collective, l'AMIAD et les acteurs industriels de la BITD se positionnent comme des leaders responsables, capables d'innover tout en accompagnant leurs ingénieurs vers l'excellence permettant ainsi de proposer des capacités innovantes à base d'IA pour les opérations terrestres.

[16] European Trustworthy AI Association (ETAIA) est une organisation à but non-lucratif créée en 2025 pour fédérer l'écosystème européen autour de l'IA responsable et industrielle. Elle découle du programme Confiance.ai (financé dans le cadre de France 2030) et vise à faciliter la conception, la validation et le déploiement de systèmes d'IA fiables, explicables et conformes aux réglementations européennes. Ses missions sont de promouvoir l'IA de confiance en fournissant une méthodologie d'ingénierie et des outils open-source de pointe ; d'accélérer la conformité aux exigences de l'AI Act et d'autres cadres réglementaires ; de créer un écosystème européen réunissant grandes entreprises incluant des industriels français (Air Liquide, Airbus, KNDS, MBDA, Naval Group, Safran, Sopra Steria, Thales), PME, startups comme Numalis, laboratoires de recherche, universités, organismes de régulation et organisations de certification et de soutenir l'autonomie européenne en matière d'innovation responsable en IA.

5. Annexes : Acronymes

AMIAD	Agence Ministérielle pour l'IA de Défense
ATDR	Automatic Target Detection and Recognition
BITD	Base Industrielle et Technologique de Défense
C2	Command and Control
CNN	Convolutional Neural Networks
CSP	Programmation par contraintes
ConOps	Concept of Operations
DH	Direction des Hébergements
DRI	Détection, Reconnaissance, Identification
EAR	Export Administration Regulations
GINN	Geometric Informed Neural Network
GNSS	Géolocalisation et Navigation par un Système de Satellites
GOFAI	Good Old-Fashioned AI
IA	Intelligence Artificielle
IHM	Interfaces Humain-Machine
IR	Infra Rouge
ISR	Intelligence, Surveillance, Reconnaissance
ISTAR	ISR + Target Acquisition
ITAR	International Traffic in Arms Regulations
IVVQ	Intégration, Vérification, Validation, Qualification
LLM	Large Language Model
M2MC	Multi-Milieux Multi-Champs
MDO	Multi Domain Operation
MEDOT	Méthode d'Elaboration d'une Décision Opérationnelle Tactique
OODA	Observer, Orienter, Décider, Agir
ORTAC	Operational Resource and Tactical Action Control
PINN	Physics Informed Neural Network
ROEM	Renseignement d'Origine ElectroMagnétique
TRL	Technology Readiness Level

Quand l'excellence devient **VITALE**

Groupement des industries françaises de défense et de sécurité terrestres et aéroterrestres

39 rue Mstislav Rostropovitch
75017 Paris
+33 (0)1 44 14 58 20
contact@gicat.fr

gicat.com