Le Groupement des industries françaises de défense et de sécurité terrestres et aéroterrestres (GICAT) publie un rapport collectif de 53 pages consacré à l'intelligence artificielle appliquée aux opérations terrestres. Rédigé par un groupe de travail réunissant des représentants de Safran, Thales, Arquus, MBDA, KNDS France, Bertin Technologies et Numalis, le document se présente comme un plaidoyer en faveur d'une intensification de l'usage de l'IA par les forces terrestres françaises. Sa thèse centrale tient en une phrase : l'IA n'est plus une option prospective, son déploiement opérationnel est devenu critique. Six ans après un précédent rapport du GICAT daté de 2020, les auteurs dressent un constat d'urgence et formulent des recommandations à destination des armées, de l'État et de la base industrielle et technologique de défense (BITD).

Un contexte militaire profondément transformé

Le rapport s'ouvre sur l'analyse d'un environnement opérationnel en mutation rapide. Les conflits récents, en premier lieu la guerre en Ukraine, ont mis en évidence plusieurs phénomènes structurants : la densification et l'accélération des menaces, la prolifération de drones à bas coût assemblés à partir de composants civils, la saturation des champs de bataille et le raccourcissement des cycles de développement et de contre-mesures, désormais comptés en mois. Selon les auteurs, cette « *guerre des ingénieurs* » a nivelé les rapports de force et rendu partiellement obsolète la supériorité technologique traditionnelle des armées occidentales.

Dans ce contexte, le document identifie six dimensions où l'IA apporte une contribution distinctive : la transparence du champ de bataille, grâce au traitement de masses croissantes de données hétérogènes ; le déni d'accès, en permettant aux plateformes d'opérer dans des conditions de brouillage GNSS et de communications dégradées ; la vitesse, par l'automatisation de fonctions réflexes et l'accélération de la boucle OODA (observer, orienter, décider, agir) ; la collaboration entre machines et entre échelons ; la masse, un opérateur unique pouvant gérer une multiplicité de vecteurs ; et la létalité, via un ciblage plus rapide et plus précis. Le rapport souligne qu'un retard dans la mise en œuvre de ces capacités peut « modifier substantiellement le rapport de forces et changer le sort de la bataille ».

Le document prend soin de définir son vocabulaire, distinguant la donnée (élément brut non interprété), l'information (donnée mise en contexte) et la connaissance (résultat d'une réflexion s'appuyant sur un référentiel collectif, généralement propre à un métier).

11 cas d'usage recensés

Le cœur du rapport recense 11 applications opérationnelles, présentées selon une grille commune : capacités visées, type d'IA mobilisé, valeur ajoutée et conditions de montée en maturité.

La détection radar de menaces aériennes ouvre la liste. Face aux drones à faible signature radar et aux attaques saturantes, l'IA statistique et connexionniste aide les opérateurs à discriminer un drone parmi des objets lents comme les oiseaux. Les radars de surface de Thales, d'une portée de 250 à plus de 500 km, embarquent des algorithmes d'apprentissage

profond présentés comme fiables et explicables. Le plein potentiel passerait par un réseau collaboratif de capteurs fixes, mobiles et aéroportés, la fusion radar-optronique-acoustique et l'analyse des signatures micro-Doppler.

La détection optronique constitue le deuxième cas. Avec des munitions téléopérées atteignant 400 km/h, le délai entre apparition d'une menace à l'horizon et frappe éventuelle se réduit à 30-45 secondes. Les modèles de détection, reconnaissance et identification (DRI), construits par apprentissage profond, équipent ou équiperont des matériels comme les viseurs PASEO et boules Euroflir de Safran, ou la caméra CamSight AI de Bertin Technologies, qui réalise une reconnaissance de cibles en imagerie thermique avec une consommation d'environ 4 watts. Le rapport identifie trois lignes d'action : bases de données étatiques et industrielles pour pallier la rareté de la donnée réelle, algorithmes frugaux en calcul pour l'embarquabilité, et principes partagés d'intégration.

L'établissement d'une situation tactique à partir de drones ISR forme le troisième cas d'usage. Les solutions évoquées couvrent la navigation résiliente en l'absence de GNSS, la localisation d'émetteurs adverses par traitement des signaux radiofréquence, et la DRI sur flux optroniques, à l'image de la famille ODIN de Safran.AI ou du système SwarmMaster de Thales pour l'opération d'essaims. L'enjeu principal réside désormais dans la convergence de ces briques élémentaires ; le projet Pendragon, engagé en 2025 avec l'AMIAD (Agence ministérielle pour l'IA de défense), doit développer un C2 pour une unité intégralement dronisée.

La prise de décision en environnement classifié illustre l'apport de l'IA aux postes de commandement. Le rapport cite la plateforme souveraine ARTEMIS.IA, développée par ATHEA, et l'assistant ANTICIPE de Thales. Les objectifs chiffrés annoncés sont ambitieux : réduire le cycle décisionnel de 24 heures à quelques minutes, traiter cent fois plus d'informations à effectif constant, réduire de 30 % le temps de formation des opérateurs. Lors de l'exercice OTAN Steadfast Jupiter d'octobre 2023, un quartier général réduit de dix opérateurs équipés d'ANTICIPE aurait rivalisé avec le QG de Brunssum et son millier d'opérateurs. Le rapport note toutefois que l'IA générative, utile pour rédiger des synthèses, « *peut halluciner* », ce qui impose de garantir la validité opérationnelle des contenus générés.

Suivent la réduction de la charge cognitive, avec la suite DigitalCrew de Thales, déjà partiellement déployée sur le véhicule britannique Ajax et prévue sur le Challenger 3, et également utilisée dans des contextes civils de lutte anti-braconnage au Botswana ; les véhicules automatisés et la robotique, à travers les programmes FURIOUS (Safran), DROIDE (KNDS et Safran) et les travaux d'Arquus sur le suivi de chemins par réseaux de neurones, entraînés sur quelques milliers d'images, avec pour défi suivant l'inférence de la « *traficabilité* » des terrains ; l'aide à la conception de la manœuvre, où l'outil ORTAC de Safran combine programmation par contraintes et techniques neuro-symboliques pour planifier les déplacements coordonnés d'unités multiples.

La maintenance prédictive fait l'objet d'un développement substantiel : l'hybridation entre IA symbolique (modèles AMDEC, arbres de défaillance) et IA connexionniste (analyse de séries temporelles issues de capteurs) permet d'estimer la durée de vie restante des équipements et d'identifier les causes racines des anomalies, l'IA générative venant en appui pour guider les techniciens et automatiser les comptes rendus. La logistique militaire bénéficie d'apports

comparables : anticipation des besoins, optimisation d'itinéraires sous contraintes dynamiques, ravitaillement autonome en zone hostile, détection de cybermenaces sur les chaînes d'approvisionnement.

L'entraînement et la simulation s'appuient sur le projet européen Battleverse, financé par le Fonds européen de défense, qui vise la génération « *à la demande* » de jumeaux numériques du champ de bataille au moyen d'une IA générative neuro-symbolique. Enfin, la détection rapide de munitions rôdeuses pour l'autoprotection « *soft kill* » des blindés repose sur des réseaux de neurones analysant des flux infrarouges, l'intégration de l'IA directement dans la caméra limitant la surface d'attaque du système.

Trois paradigmes d'IA, une cartographie des supériorités

La partie méthodologique du rapport adopte une démarche pédagogique revendiquée, visant à « *démythifier* » l'IA. Elle distingue deux courants historiques : l'IA symbolique ou à base de connaissances (la « *GOFAI* »), fondée sur la manipulation de règles logiques explicites, transparente et traçable mais fragile face aux situations imprévues ; et l'IA dirigée par les données (statistique et connexionniste), performante sur les données massives non structurées mais opaque, non déterministe et sensible à la dérive des données. L'IA générative et les systèmes multi-agents, support de l'« *agentique* », complètent le panorama. Le rapport cite David Sadek, vice-président IA de Thales : « *L'IA connexionniste est l'IA des sens, et l'IA symbolique est celle du sens.* »

Les auteurs organisent ensuite les apports de l'IA selon une hiérarchie de supériorités : supériorité de la donnée (collecte et sécurisation), informationnelle (fusion multi-sources, détection d'anomalies), de la connaissance (intégration des doctrines, des retours d'expérience et des règles d'engagement), décisionnelle (analyse prédictive, planification, gestion des ressources) et opérationnelle (apprentissage par renforcement, systèmes multi-agents, planification dynamique). Chaque niveau mobilise des paradigmes différents, l'IA hybride étant systématiquement présentée comme l'approche la plus prometteuse pour concilier adaptation et respect des cadres doctrinaux et réglementaires.

Une section détaillée traite de la gestion des données et des connaissances. Les données d'entraînement doivent être représentatives du terrain, collectées en conditions opérationnelles réelles, annotées par des personnels formés au métier, validées par des experts, sécurisées et partagées entre acteurs. Le recours aux données synthétiques et aux modèles frugaux est recommandé pour pallier la rareté des observations réelles, sous réserve de validation. Le rapport aborde également les vulnérabilités spécifiques des IA : attaques adversariales exploitant le fonctionnement des algorithmes, empoisonnement des bases de connaissances ou des données d'entraînement, dépendance aux infrastructures de communication, et risques d'inférence d'informations classifiées par croisement de bases de connaissances.

Trois réponses structurantes

Face aux limites des approches actuelles, le rapport articule trois réponses.

- **La première est l'hybridation.** Les approches neuro-symboliques combinent apprentissage automatique et raisonnement formel. Le document détaille plusieurs familles techniques : les Physics-Informed Neural Networks (PINN), qui contraignent l'apprentissage par des équations différentielles décrivant les lois physiques (Navier-Stokes, Maxwell, Fourier) ; les Geometry-Informed Neural Networks (GINN), appliqués notamment à la reconnaissance automatique de cibles sur signatures micro-Doppler ; les réseaux morphologiques profonds (DeepMorphNet) ; ou encore l'inférence floue, illustrée par le module Alpha de la start-up Psibernetix, acquise par Thales en 2019, devenu célèbre pour avoir tenu en échec des pilotes de chasse en simulation de combat aérien. L'IA hybride promet simultanément robustesse, explicabilité, frugalité en données et conformité doctrinale.
- **La deuxième réponse porte sur l'IA de confiance et la garantie des performances.** Le rapport rappelle les six exigences de l'AI Act européen — robustesse, efficacité, fiabilité, utilisabilité, interaction humain-système et contrôle humain — et souligne qu'elles prennent une forme particulièrement exigeante en défense : validation formelle voire certification pour la sûreté, auto-explication en temps réel comme condition d'acceptabilité, relation bilatérale complexe entre IA et cybersécurité. Les auteurs insistent sur la distinction entre précision et robustesse : un système précis peut ne pas être robuste, comme le montre le phénomène de sur-apprentissage.
- **La troisième réponse concerne l'intégration, l'embarquabilité et l'appropriation humaine.** Le portage de fonctions IA sur calculateurs embarqués impose des compromis de compression, de latence et de SWaP (taille, masse, puissance), et la qualification doit porter sur le comportement réel du système déployé, non sur un prototype de laboratoire. Côté facteurs humains, le rapport traite de la charge cognitive, de la téléopération, des réticences des opérationnels face à des robots perçus comme « *incontrôlables* », et pose l'explicabilité comme préalable à l'exploitation des technologies d'IA, le maintien de l'humain dans la boucle décisionnelle pour l'usage de la force létale demeurant un principe fondamental.

Souveraineté : un chapitre d'alerte

Le rapport consacre des développements étendus à la souveraineté, dressant un inventaire des dépendances françaises et européennes : infrastructures cloud et piles logicielles MLOps dominées par les acteurs américains, approvisionnement en semi-conducteurs concentré à Taïwan et en Corée du Sud, architectures de modèles inventées majoritairement dans des laboratoires américains, dont l'accès tend à se restreindre ou à devenir payant. Les réglementations extraterritoriales américaines (ITAR, EAR) sont décrites comme des leviers de pression géopolitique potentiels. Le document mentionne des initiatives de réponse, comme l'outil souverain AIDGE porté par le CEA, et appelle à investir massivement dans les organismes de normalisation (ISO, IEC, CEN-CENELEC, ETSI) et à constituer des coalitions industrielles européennes pour certifier des solutions « ITAR-free ».

Un bilan en demi-teinte et un appel à l'action

La dernière partie dresse le bilan des six années écoulées depuis le rapport de 2020. Le constat est nuancé : « *l'ambition initiale n'a été que partiellement atteinte* ». Un tableau de

maturité technologique (TRL) brique par brique montre des progressions contrastées — saut majeur pour l'apprentissage machine et l'analyse de données (de TRL 5 à 8), passées d'un usage artisanal à l'industrialisation, progression plus modeste ailleurs, le TRL 9 restant hors d'atteinte en défense pour le deep learning en raison des enjeux d'explicabilité et de certification.

Les auteurs constatent que l'innovation militaire est désormais tirée par des acteurs civils plus agiles, et que la guerre en Ukraine a démontré la capacité d'acteurs non étatiques à transposer rapidement des innovations duales. Ils en tirent une conclusion sans détour : sans volonté politique forte et coordination systémique, la France ne pourra pas rivaliser avec des compétiteurs qui intègrent l'IA à un rythme soutenu, parfois sans les contraintes éthiques ou réglementaires qui pèsent sur les démocraties.

Les recommandations finales plaident pour une approche systémique : créer des cadres d'expérimentation plus souples permettant de valider rapidement des concepts et d'itérer sans attendre une certification complète, selon une logique de qualification incrémentale ; fédérer recherche, industrie et opérationnels ; accepter un niveau de risque calculé sans renoncer aux garde-fous de sécurité et d'éthique ; développer une discipline d'« *ingénierie de l'IA de confiance* », dans la continuité du programme Confiance.ai et de structures comme l'European Trustworthy AI Association créée en 2025 ; enfin, investir dans l'attractivité des talents et l'acculturation à l'IA de l'ensemble des forces. La création de l'AMIAD et les initiatives industrielles comme cortAIx (Thales) ou Safran.AI sont citées comme des signes de prise de conscience, mais le rapport conclut que « le temps de la réflexion pure est révolu : place à l'itération rapide et à la validation terrain ».

View Fullscreen
Aller au contenu PDF