EGE Ecole de Guerre Economique

RAPPORT D'ÉTUDE

Robotisation du champ de bataille : enjeux de souveraineté pour la France

IA embarquées et autonomie décisionnelle

Cette publication s'inscrit dans le cadre du programme pédagogique du Master 2 Risques, sûreté internationale et cybersécurité – RSIC 08

Année académique 2025 — 2026

Executive Summary

1- Accroche

L'apparition des systèmes d'IA embarquée révolutionne la chaîne de commandement et de décision sur le champ de bataille. Alors qu'en pleine guerre froide en octobre 1962, treize jours ont été nécessaires afin de permettre aux dirigeants américains et soviétiques de trancher sur l'entrée du monde dans un hiver nucléaire, il ne faut désormais que quelques instants à l'IA embarquée sur les systèmes militaires pour qualifier une cible et proposer une action.

2- Problématique

Avec l'apparition de ce nouveau paradigme, un basculement majeur touche directement la façon dont la guerre est menée. Des machines disposent désormais de capacités de décision et d'analyse dépassant largement les possibilités humaines. Cette révolution redéfinit la façon dont la boucle décisionnelle fonctionne entraînant des gains, mais aussi des risques majeurs. En effet, si l'accélération de la prise de décision ainsi que l'accès à une information analysée et de qualité permettent de bénéficier d'un avantage tactique non négligeable sur son adversaire, elles entraînent aussi un basculement majeur. L'accélération du cycle de décision fait apparaître des problématiques techniques, de souveraineté, mais aussi de doctrine et d'éthique. De fait, la fiabilité des modèles d'IA embarquées est toujours légitimement soumise à débat tout comme les questions de responsabilité et de nécessité d'un contrôle humain sur la décision. Dès lors, avant de s'engager sur l'adoption et l'application de l'IA embarquée au sein des forces armées françaises, il est fondamental de se poser la question de son fonctionnement et des conditions de sa mise en œuvre optimale.

3- Solutions et réponses

L'adoption et l'application de l'IA embarquée reposent sur une solution articulée autour de trois piliers. D'abord, un traitement local de l'information via *l'edge computing* et des outils comme l'ATR, qui réduisent la latence et la charge cognitive de l'opérateur tout en préservant l'autonomie décisionnelle sur le terrain. Ensuite, une gouvernance souveraine du cycle de vie des modèles, appuyée sur un écosystème industriel français structuré (Thales, Dassault Aviation, Safran, Naval Group, MBDA, DGA) et des programmes concrets tels que Preligens, Talios ou ARTEMIS.IA, sans toutefois ignorer la dépendance persistante aux briques critiques étrangères (*GPU*, semi-conducteurs, *cloud hyperscale*). Enfin, un cadre doctrinal qui sanctuarise la décision humaine, la France plafonnant volontairement l'autonomie de ses systèmes au niveau L4 et excluant tout système d'arme létale pleinement autonome. Face à l'impossibilité de rivaliser en masse avec les États-Unis ou la Chine, la France opte pour une souveraineté ciblée : protéger les données sensibles, certifier les chaînes *MLOps* (Annexe 2), auditer les logiciels embarqués et maintenir un contrôle humain effectif là où la criticité l'exige.

4- Contexte

L'IA embarquée s'inscrit dans un contexte de compétition technologique soutenue entre les puissances militaires étatiques, notamment les États-Unis, la Chine et les puissances européennes. Elle concerne l'utilisation de systèmes technologiques robotisés et connectés à un *Large Langage Model* (*LLM*). En France, cette dynamique mobilise la BITD française, ainsi que la DGA et l'Agence de l'Innovation de Défense (AID). Toutefois, cet effort industriel reste contraint par des dépendances critiques aux semi-conducteurs, *GPU*, *cloud hyperscale*, logiciels propriétaires, modèles de fondation et outils *MLOps* souvent contrôlés hors du périmètre européen.

5- Différenciation

La position française sur les systèmes d'IA embarquée se distingue juridiquement par le refus de déléguer à une machine la décision de vie ou de mort. Contrairement à une logique de pleine autonomie, l'approche française privilégie des systèmes intégrant de l'autonomie, mais placés sous contrôle humain. Elle se différencie également par sa logique de souveraineté sélective : Il ne s'agit pas de tout produire seul mais d'identifier les dépendances critiques, de sécuriser les données sensibles, d'auditer les algorithmes, de certifier les chaînes *MLOps*, de renforcer la cybersécurité embarquée et de garantir la capacité humaine à contester ou interrompre une recommandation algorithmique.

6- Idées fortes

L'analyse conduit à quatre constats majeurs. Premièrement, la nécessité de privilégier la fiabilité à la vitesse de décision, la performance de l'IA embarquée dépendant avant tout de la qualité des données d'entraînement et de la robustesse des capteurs face au terrain ; elle n'est pas infaillible.

Deuxièmement, la dépendance à la qualité de la donnée pour garantir la performance d'une IA embarquée devient un enjeu essentiel. Dès lors, bénéficier d'une donnée souveraine et de qualité est primordial afin de construire un modèle d'IA embarqué indépendant et robuste. De la même manière, la maîtrise du cycle de vie des modèles (*MLOps*) est une prérogative conditionnant l'indépendance opérationnelle des armées.

Troisièmement, la protection des transmissions constitue un impératif central, la connectivité hybride sur laquelle repose l'IA embarquée restant exposée aux risques d'interception, de brouillage et de rupture post-quantique.

Enfin, au-delà du technique, se pose un risque cognitif et éthique de déréalisation du combat : Face à ce risque, la France opère aujourd'hui un choix doctrinal assumé en plafonnant volontairement l'autonomie de ses systèmes au niveau L4 (Annexe 4).

Recommandations

1. *Entraîner les IA en conditions réelles* en enrichissant les bases d'entraînement avec des données de terrain et systématiser les tests en conditions dégradées (météo, brouillage, capteurs partiellement obstrués) permettrait de limiter concrètement le risque de *distribution shift* (Annexe 2). Les modèles gagneraient ainsi en fiabilité une fois confrontés aux situations imprévisibles du champ de bataille.

2. *Renforcer la fusion des capteurs* en multipliant et en croisant davantage les sources de données (radar, *LiDAR*, sonar, caméras) accroîtrait la redondance du système. Cette architecture réduirait directement les taux de faux positifs et négatifs, tout en limitant l'impact d'une défaillance ou d'une attaque ciblant un capteur isolé.

3. *Diversifier les canaux de télécommunication* et instaurer un audit régulier de leur intégrité permettrait de répondre à la vulnérabilité des liaisons face au brouillage ou à l'interception. Le recours accru aux constellations satellites en orbite basse (*LEO*), en pleine expansion, garantit par ailleurs une connectivité continue et à faible latence.

4. *Renforcer l'autonomie des systèmes* en développant des outils capables de fonctionner de manière autonome, sous réserve d'un encadrement strict par des règles d'engagement prédéfinies, atténuant les conséquences d'une perte de signal. Cette autonomie renforcée diminuerait la dépendance opérationnelle aux télécommunications, identifiée comme un point de fragilité majeur.

5. *Sécuriser la chaîne d'approvisionnement* en renforçant la souveraineté sur l'ensemble de la chaîne (gouvernance des données, innovation technologique, accès aux matières premières critiques) et en encadrant les partenariats sur les technologies *edge*.
6. *Développer des indicateurs d'incertitude* en accompagnant chaque suggestion algorithmique d'un indice de confiance permettrait à l'opérateur d'évaluer le risque d'erreur avant de valider une décision. Cet outil limiterait le biais d'automatisation en restaurant un véritable esprit critique dans la chaîne décisionnelle.

7. *Sanctuariser la décision humaine* en maintenant un contrôle humain réel, et non purement formel dans l'emploi des systèmes d'IA à vocation létale reste essentiel pour prévenir les risques éthiques, techniques et opérationnels. Une présence humaine

assurée prioritairement au plus près du terrain éviterait la déshumanisation du combat et préserverait la responsabilité morale et juridique de la décision.

Table des matières :

I.Introduction

L'IA embarquée est devenue un enjeu crucial du théâtre d'opération : Elle représente un outil de puissance dans un contexte de concurrence technologique acharnée entre compétiteurs stratégiques. La montée en puissance de l'IA dans les systèmes d'armes offre la possibilité, par ses capacités autonomes, de gagner en réactivité et en résilience dans un environnement de combat complexe. Toutefois, cela induit de nombreux défis concernant la souveraineté, l'autonomie décisionnelle et le financement technologique. Dans quelle mesure l'IA embarquée se situe-t-elle à la frontière entre assistance à la décision et autonomie décisionnelle militaire ? Quelles sont les limites techniques, éthiques et juridiques à un tel modèle ?

Après avoir défini la manière dont les systèmes d'IA embarqués fonctionnent et sont mis en œuvre (collecte et traitement de la donnée), la nécessité d'une donnée souveraine et crédible pour attester de sa fiabilité (maîtrise du cycle de la donnée) sera exposée. La question cruciale de la convergence de la connectivité et de la cybersécurité des systèmes d'information constitue également un facteur inhérent à son intégrité. Une seconde partie s'attachera à étudier les limites techniques, juridiques et éthiques à de tels systèmes dont l'enjeu est la souveraineté même de la France.

II.Les technologies de captations d'informations et d'aide à la décision

i.La captation de données au service de l'IA embarquée et de la décision

A. Les modules de traitement de données embarqués

De nombreuses technologies concourent à la collecte de données ; ces innovations et investissements dans la défense se concentrent sur la mise en place d'IA embarquées. Le *Edge computing* (Annexe 2) notamment, permet une aide immédiate à la décision en traitant les éléments directement à la source, sans transiter par un serveur distant, ce qui réduit la latence et permet l'émergence de systèmes autonomes, comme les drones ou les véhicules blindés.

Intégré aux drones ISR (*Intelligence, Surveillance, Reconnaissance*) chargés de la surveillance de zone, le *Edge computing* ne remonte que l'information pertinente, allégeant la bande passante, réduisant le temps de la boucle décisionnelle et la charge cognitive de l'opérateur, tout en limitant l'impact d'une coupure des liaisons. Les modules *Edge* ne sont pas les seules solutions embarquées autonomes, d'autres outils ou algorithmes, comme l'ATR (*Automatic Target Recognition*), chargé de la reconnaissance de cible, qui équipe notamment des systèmes de défense sol-air ou des radars, permettent une détection des menaces, ainsi que leurs classifications. Il s'avère efficace pour le guidage de précision de missile, mais

également dans un rôle de réduction de la charge de données à traiter sur le champ de bataille. C'est donc également un outil réduisant la pression sur les opérateurs.

B. La centralisation des données de terrains

Les capteurs de terrain non autonomes sont également essentiels à la prise de décision. Ils permettent, après une centralisation des informations, une prise de décision cohérente et claire. Par exemple, le système d'Information de Combat SCORPION (Synergie du Contact Renforcé par la Polyvalence et l'Info valorisation), regroupe de multiples capteurs pour offrir aux postes de commandement la connaissance d'une situation tactique consolidée. Les capteurs de données et l'intégration d'IA sont donc des moyens d'obtenir des renseignements fiables et exploitables facilement, afin de récupérer un avantage sur le champ de bataille.

Cette centralisation nécessite des capteurs variés : le *LiDAR*, utile à la cartographie et à la détection d'objets dissimulés; les satellites, indispensables à la connaissance géographique du champ de bataille, à l'image des radars; ou les sonars pour la surveillance marine. L'IA permet une classification automatique et en temps réel des cibles et contacts détectés, que ce soit pour les radars AESA (ajustement en temps réel de la fréquence, résilience accrue) ou pour le sonar 76Nano de Thalès (réduction du risque d'erreur et du temps de décision face à une menace sous-marine).

C. L'émergence des données humaines

Enfin, les nouvelles technologies et le développement d'IA permettent l'émergence de nouvelles sources de données servant la prise de décision. L'étude du facteur humain se développe, se référant à l'état cognitif du soldat. La France s'intéresse notamment aux électroencéphalogrammes (EEG) afin de récupérer l'état de fatigue et l'état de surcharge des pilotes, car cette technologie repose sur la captation via des électrodes, de l'activité électrique générée par les neurones.

D'autres recherches sont en phase de développement, comme les interfaces cerveau-machine (ICM, ou *BCI* en anglais), portées notamment par l'armée américaine ainsi que par des entreprises comme Neuralink. Elles pourraient permettre la détection automatique de menaces et le contrôle d'engins par réduction du temps de latence entre intention et action, renforçant ainsi les capacités des soldats tout en réduisant leur exposition au danger.

Cet intérêt se traduit par des recherches croissantes, comme le projet européen NEUROQUAD, qui étudie depuis 2024 des technologies d'IA pour la surveillance cognitive des pilotes en temps réel. La prise en compte des données humaines devient ainsi un enjeu d'avenir pour les armées, au même titre que la captation des informations de terrain.

ii. Contrôle et usage des données : un enjeu stratégique de souveraineté

L'intelligence artificielle embarquée ne produit aucune décision autonome sans données fiables, correctement traitées et continuellement mises à jour. La véritable souveraineté française repose donc sur la maîtrise du cycle de vie des données militaires : leur traitement, leur gouvernance, leur validation et leur exploitation opérationnelle.

A. Le traitement embarqué des données : transformer l'information en décision opérationnelle

À bord des systèmes autonomes, l'information issue de capteurs multiples (caméras, radar, *LiDAR*, sonar) est fusionnée, nettoyée, filtrée puis hiérarchisée afin de devenir exploitable (Annexe 2). C'est de ce traitement que découlent la détection de cibles, la classification, la reconnaissance d'objets, l'estimation des menaces, la navigation autonome et la priorisation des objectifs. C'est dans ce contexte que la latence est déterminante, la décision devant souvent être prise instantanément. Si ce traitement dépend d'une infrastructure ou de logiciels étrangers, la France perd la maîtrise de sa propre chaîne décisionnelle.

B. Gouvernance du cycle de vie des modèles : MLOps militaire comme enjeu de souveraineté

La souveraineté ne dépend pas seulement du développement de l'IA, mais aussi de sa maintenance dans la durée. Le cycle de vie complet en deux phases (pré/post déploiement) d'un modèle (Annexe 1) soulève des questions essentielles, telles que l'entraînement des modèles, le stockage des données, la validation des performances, la modification des algorithmes. Le manque de contrôle sur ces différentes étapes entraîne des risques de dépendance à des plateformes *cloud* ou à des logiciels étrangers, l'impossibilité d'auditer des modèles propriétaires, de porte dérobée et de perte de contrôle sur l'évolution des capacités militaires. Le *MLOps* devient ainsi une infrastructure stratégique comparable à une chaîne logistique de défense.

C. Qualité, robustesse et confiance dans les modèles d'IA embarqués

La valeur des données va dépendre en dernier ressort de la fiabilité des modèles qui les exploitent. Elles se regroupent sous deux axes : technique (vision artificielle, détection de cibles, classification, navigation) et analytique (fusion des données, diagnostic ou aide à la décision). Leur performance s'évalue à travers la précision, les taux de faux positifs et négatifs, l'explicabilité, ainsi que la robustesse face aux perturbations. Une IA imprécise peut identifier un civil comme cible, manquer une menace réelle ou dégrader l'ensemble de la chaîne de commandement. La maîtrise des modèles garantit des performances conformes aux exigences opérationnelles françaises, sans dépendre de standards imposés par des acteurs étrangers.

iii. Connectivité et cybersécurité de l'IA embarquée militaire

A. Connectivité : la nécessité d'une architecture hybride

L'intelligence artificielle embarquée dans les systèmes militaires repose sur une infrastructure largement invisible (calcul embarqué, liaisons satellitaires, *cloud*, mises à jour logicielles, contrainte de bande passante) qu'il faut sécuriser dans un contexte spécifique : un adversaire actif qui cherche à intercepter ou brouiller les liaisons, une mobilité permanente des unités, une instabilité des connexions, et des enjeux souvent vitaux et immédiats.

Pour le combat collaboratif, les armées ont fait le choix de l'hybridation des réseaux militaires et commerciaux afin de gagner en diversification, en résilience et en indépendance. Ainsi, le programme satellitaire géostationnaire Syracuse IV est associé à des constellations civiles en orbite basse (*LEO*) plus proches de la Terre afin de réduire la latence de connectivité. C'est l'exemple du contrat Centaure (juin 2026) que la France a signé avec Eutelsat pour un accès garanti à une partie de la constellation OneWeb (Annexe 5). L'intérêt de ce contrat dépasse la seule question de l'accès satellite : il finance également le durcissement de la cybersécurité des flux transmis. Ce cas est un exemple de la nécessité de faire converger à la fois les enjeux de connectivité et de cybersécurité. Sur le segment terrestre, cette même logique d'hybridation se retrouve avec la 5G militaire dans le but de connecter localement drones et capteurs sur des sites fixes sans dépendre du satellite. Toutefois, malgré des projets pilotes européens, les limites sont encore nombreuses : retard d'adoption, risques d'espionnage et de manipulation réseau.

B. La cybersécurité des systèmes embarqués : un besoin d'exigences spécifiques

Le risque de cyberattaques sur les drones ou les satellites est désormais devenu une réalité (exemple en 2020 de l'attaque russe contre le satellite KA-SAT de Viasat). Ainsi, toute architecture de connectivité ne peut se penser indépendamment de sa sécurisation. La cybersécurité des systèmes embarqués (Annexe 2), nécessite un renforcement des mesures de cybersécurité classiques (chiffrement de bout en bout, authentification forte des nœuds, *etc.*) et des mesures propres, comme la résilience à la déconnexion (DIL - *Denied, Intermittent, Limited*), des mécanismes de zeroization (effacement d'urgence des données), de segmentation de l'information ou encore de protocoles anti-brouillage. Cette exigence de sécurité suppose également un cadre d'homologation rigoureux, à travers l'établissement de standards de certification, d'audit et de traçabilité des systèmes déployés.

C. Des défis à long terme : l'exemple du post-quantique

À plus long terme se profile un nouveau défi: la rupture post-quantique et la menace du *harvest now, decrypt later*, (*HNLD*) ou la capacité à stocker des données chiffrées qui ne pourront être déchiffrées qu'une fois l'ordinateur quantique suffisamment mature. La stratégie retenue par l'Agence Nationale de la Sécurité des Systèmes d'Information (ANSSI)

repose sur une hybridation cryptographique avec pour cibles prioritaires les opérateurs d'importance vitale (OIV). En effet, l'ANSSI a déclaré ne plus accepter, à partir de 2027, de produits de sécurité qui n'intègrent pas de cryptographie post-quantique.

III. Les enjeux éthiques et techniques

i. La vulnérabilité des capteurs comme facteur de fragilisation des systèmes autonomes

A. Le risque d'une exhaustivité imparfaite des modèles d'entraînement

Les modèles d'apprentissage sont le point de départ d'une utilisation efficace de l'IA embarquée sur un théâtre d'opération, mais ils en sont aussi la première limite. Ces modèles sont un élément central des capacités de perception et d'aide à la décision, permettant la contextualisation de l'environnement et l'interprétation de l'information reçue. Concrètement, l'entraînement de ces modèles repose aujourd'hui sur la qualité, la diversité et la représentativité des données d'entraînement. Cette approche présente une limite majeure. Les données rencontrées sur le théâtre d'opérations peuvent différer significativement de celles utilisées lors de l'entraînement. Ce phénomène, appelé *distribution shift* (Annexe 2), entraîne une baisse des performances du modèle lorsque celui-ci est confronté à des situations inédites ou mal représentées durant son apprentissage. Cela peut conduire à une mauvaise interprétation de l'environnement, à une diminution de la fiabilité de la détection ou de la classification des cibles, donc à une dégradation de la qualité de la décision automatisée ou des suggestions de décision.

B. La vulnérabilité des capteurs : talon d'achille technique de l'automatisation par IA

Comme l'a démontré notre point précédent, la complétude de la donnée acquise par les systèmes d'IA embarquée est primordiale à son bon fonctionnement et surtout à sa fiabilité. Or, toute information exploitée par les systèmes d'IA embarquée repose sur un ensemble de capteurs vulnérables aux conditions du théâtre opérationnel. La météo, la guerre électronique ou encore les dommages physiques aux matériels peuvent entraîner une déperdition de l'information et de la donnée. Cela conduit les systèmes d'IA embarqués à

devoir transmettre des propositions ou prendre des décisions qui sont erronées. La fusion des capteurs (Annexe 2) tente de pallier ce problème en limitant les faiblesses de chacun. Cependant, lorsqu'ils sont simultanément perturbés, cette fusion ne suffit plus.

C. Les attaques adversariales : cheval de Troie de l'instrumentalisation des systèmes d'IA embarqué

Dans la même logique que pour les risques inhérents aux données d'entraînement, les données captées par les systèmes d'IA embarquée, peuvent aussi être instrumentalisées ou détournées par la partie adverse afin de rendre la prise de décision par IA inopérante ou faussée. Les attaques adversariales (Annexe 2) sont une manière de tromper l'IA par des modifications minimes sur les équipements. Dès 2017, le *MIT* avait pu démontrer qu'en concevant délibérément une optimisation mathématique sur une texture appliquée à un objet 3D cela permettait à un modèle IA spécifique de la classer à tort comme un fusil. Pour cet exemple, une impression de carapace de tortue dont seulement la texture avait été modifiée délibérément, avait suffi à ce que l'IA la classifie comme un fusil, alors que son aspect général n'avait pas fondamentalement divergé de celui d'une carapace de tortue (annexe 3).

D. Les systèmes de télécommunication : interface indispensable entre IA embarquée et décideurs humains

L'un des objectifs de l'architecture des systèmes avec IA embarquée est de réduire la dépendance aux infrastructures extérieures dont les systèmes *GPS* ou de télécommunication. Cependant, dans les architectures militaires contemporaines, les télécommunications demeurent essentielles pour assurer le partage de la situation tactique, la coordination entre les différentes plateformes, ou encore la transmission des ordres. Ce point est d'autant plus important que dans la plupart des doctrines occidentales les décisions relatives à l'emploi de la force nécessitent une validation humaine. Ainsi, si l'IA peut continuer à fonctionner localement en cas de perte des communications, il n'empêche que ses capacités opérationnelles globales sont, elles, fortement dégradées.

ii. Evolution du commandement, risques létaux et éthique

L'autonomie décisionnelle (Annexe 2) désigne « *l'aptitude d'un système informatique à interpréter son environnement et à choisir une ligne d'action parmi plusieurs options possibles, sans intervention humaine directe* » (Comité d'éthique de la défense, 2021).En droit français, les Systèmes d'armes létaux autonomes (SALA) (Annexe 4) sont juridiquement inexistants et interdits de développement : la position de la France, dictée par son adhésion aux Conventions de Genève, exclut constitutionnellement de déléguer à une machine la décision de vie ou de mort.

A. Ethique et sécurisation du commandement face à l'hyper-vitesse du combat

Le premier défi réside dans la préservation d'un commandement éthique face à la compression extrême du temps, afin de prémunir les forces armées contre les tirs létaux illégitimes et les exactions opérationnelles. L'IA embarquée la plus avancée dans nos armées reste strictement cantonnée au cadre des systèmes intégrant de l'autonomie (SALA), où l'homme conserve la maîtrise exclusive du feu. L'IA désigne et aide, mais ne décide pas. L'IA bouleverse la boucle doctrinale OODA (*Observer, Orienter, Décider, Agir*) en réduisant drastiquement le temps d'élaboration d'une solution. L'IA excelle à traiter les phases d'observation (fusion des capteurs) et d'orientation (tri automatique des menaces). En compressant ces deux étapes en quelques instants, elle réduit considérablement le délai entre la perception d'une cible et l'action de feu. Le goulot d'étranglement se situe désormais au moment du décider. Face à des attaques hyper-véloces, le risque majeur est le « saut algorithmique » (Centre de doctrine et d'enseignement du commandement, 2023), où l'opérateur est poussé à une action réflexe, transformant le contrôle humain en une simple validation notariale d'un tir déjà calculé par la machine.

Conformément à la Stratégie d'IA de Défense et à l'avis du Comité d'éthique de la défense du 29 avril 2021, le maintien officiel de l'humain dans la boucle est l'unique rempart contre les violations du droit international humanitaire. Une machine est incapable d'évaluer juridiquement les principes conventionnels de distinction, de nécessité et de proportionnalité d'une riposte. L'éthique du commandement impose que l'humain reste le filtre moral pour identifier un abandon de combat, un civil ou un otage, évitant ainsi des ouvertures du feu aveugles s'apparentant à des crimes de guerre.

Le combat connecté via les drones *Reaper*, les futurs *Patroller* ou les effecteurs du programme SCAF introduit une déréalisation du front à travers des écrans (Comité d'éthique de la défense, 2021). Si cette distance physique peut atténuer la perception humaine de la gravité de l'acte de tuer, elle s'accompagne paradoxalement d'un voyeurisme macabre. Devoir observer en haute définition et pendant des heures les dommages corporels après une frappe (*Battle Damage Assessment*) génère de graves traumatismes psychologiques (Service de santé des armées, 2022). La sanctuarisation de la décision humaine protège ainsi le soldat contre la déshumanisation du combat.

B. Fiabilité du référentiel universel et neutralisation des biais algorithmiques

Le second défi est purement technique et architectural : Il s'agit de garantir la justesse absolue de la donnée pour préserver la liberté de choix du chef militaire et empêcher la machine d'influer insidieusement sur la décision de tir.

Pour que les capteurs des armées coopèrent efficacement, toutes les données doivent être projetées sur un référentiel universel et standardisé (mêmes repères géospatiaux, mêmes formats d'horodatage). Si l'IA d'un drone éclaireur et le système d'artillerie d'un blindé ne partagent pas exactement la même grammaire numérique, le système produit des erreurs

de ciblage, selon la DGA. Ce standard universel est indispensable pour que la donnée transmise soit techniquement juste, neutre et exempte de toute distorsion technique pouvant provoquer une erreur.

L'enfermement informationnel demeure le piège le plus important pour la chaîne de commandement. L'IA va orienter indirectement la décision par le tri qu'elle opère. L'algorithme facilite le travail en proposant certaines solutions, en masquant certaines données jugées non prioritaires, ainsi qu'en ne labellisant pas une menace asymétrique, comme un véhicule civil modifié. Cependant, il prive l'opérateur de l'accès à la réalité du terrain. L'humain subit alors un biais d'automatisation (Agence ministérielle pour l'IA de défense [AMIAD], 2024) : il valide les suggestions de la machine par manque de visibilité globale. Le référentiel unique doit au contraire garantir que l'IA restitue une donnée transparente et explicable, permettant au chef militaire de décider en totale liberté de conscience, sans subir la logique ou les angles morts de l'algorithme.

iii. Souveraineté, *MLOps* militaire et rapports de force industriels

A.Une montée en puissance française encore dépendante des chaînes de valeur étrangères

Les parties précédentes ont montré que l'IA embarquée dépend de données fiables, d'un traitement rapide et d'un contrôle humain. La souveraineté prolonge directement cet enjeu car posséder un système militaire équipé d'IA ne suffit pas si les couches systémiques (techniques, logicielles et industrielles) qui assurent son fonctionnement échappent au contrôle national ou européen. Capteurs, données, modèles, logiciels embarqués, cloud, semi-conducteurs, *MLOps* doivent être sous contrôle pour maîtriser un système d'IA. La France continue de progresser dans l'intégration de l'IA militaire : TAIIA/Preligens pour le renseignement d'image, Talios sur Rafale, SkyView et ANTICIPE pour le commandement, Pathmaster pour la guerre des mines, SearchMaster pour la patrouille maritime, CoHoMa pour les essaims drones-robots et ARTEMIS.IA pour le traitement massif des données. Cette dynamique s'appuie sur un écosystème de la BITD française, d'acteurs institutionnels notamment la DGA, l'AID et ainsi que sur un tissu de plusieurs startups spécialisées.

B. Des dépendances critiques qui déplacent la souveraineté vers les couches invisibles

Cependant, cette montée en puissance reste partielle. Les briques critiques de la chaîne de valeur de l'IA (*GPU*, fonderies avancées, *clouds hyperscale*, bibliothèques logicielles, modèles de fondation et outils *MLOps*) restent largement contrôlées par des acteurs domiciliés hors de la France et souvent hors de l'Europe. À titre d'exemple, l'Union européenne ne représente qu'environ 10 % du marché mondial des semi-conducteurs, tandis que plus de 90 % des modèles d'IA les plus utilisés seraient américains ou chinois. Le paradoxe est donc clair : les armées françaises intègrent de plus en plus l'IA mais une partie des conditions industrielles qui rendent cette IA possible reste située hors du périmètre de

souveraineté national ou européen. La souveraineté ne peut donc pas être évaluée au seul niveau du système final. Un équipement assemblé en France peut dépendre d'un semi-conducteur étranger, d'un *framework* américain, d'un modèle entraîné hors Europe ou d'un outil *MLOps* hébergé à l'étranger. Ces dépendances exposent les armées à plusieurs risques notamment à un verrouillage technologique, de l'extraterritorialité juridique, de la fuite de données sensibles, de sabotage par mise à jour compromise, d'interruption de service ou de perte de contrôle sur le comportement du modèle.

C. Le *MLOps* comme infrastructure critique d'une souveraineté

Le *MLOps* devient alors une infrastructure de souveraineté. Il permet de maîtriser tout le cycle de vie d'un système d'IA embarqué (Annexe 1). Celui qui contrôle les données d'entraînement, les métriques de validation et les pipelines de mise à jour contrôle une partie de la décision opérationnelle. Sans *MLOps* souverain et auditable, l'IA embarquée devient une boîte noire tactique dans une chaîne de décision stratégique. Enfin, la souveraineté doit être reliée au contrôle humain. La France refuse de déléguer à une machine la décision de vie ou de mort mais le risque réside aussi d'une autonomie progressive de l'IA par la classification des données, le filtrage, la priorisation et la recommandation de l'action à mener. L'humain reste officiellement dans la boucle mais peut être capturé et saturé par la vitesse et l'autorité statistique de la machine. La souveraineté implique donc de conserver la capacité de comprendre, de contester et si nécessaire, d'interrompre la recommandation algorithmique en situation opérationnelle.

La France ne pourra pas rivaliser avec les États-Unis ou la Chine d'un point de vue quantitatif. Son espace stratégique est celui d'une souveraineté ciblée : protéger les données sensibles, certifier les chaînes *MLOps*, auditer les logiciels embarqués, sécuriser les capteurs, développer des modèles spécialisés et maintenir un contrôle humain effectif. La souveraineté algorithmique ne signifie pas tout produire seul ; elle consiste à connaître son niveau de dépendance, les acteurs qui les structurent et les encadrent, leur niveau de criticité et les capacités de rupture disponibles en cas de crise.

IV. Conclusion

L'intelligence artificielle embarquée transforme la captation de données et l'aide à la décision militaire, du niveau tactique jusqu'aux données humaines. Cette dépendance technologique fait de la maîtrise du cycle de vie des données un enjeu de souveraineté, face aux risques de dépendance étrangère et de vulnérabilité cyber. Cependant, l'automatisation reste limitée par le *distribution shift*, la vulnérabilité des capteurs et les attaques adversariales. Sur le plan éthique, la compression du temps décisionnel et les biais d'automatisation obligent au maintien d'un contrôle humain réel. L'avenir des armées reposera donc sur l'équilibre entre performance technologique, souveraineté et sanctuarisation du jugement humain.

V. Bibliographie

Agence ministérielle pour l'IA de défense. (2024). *Stratégie IA*. https://www.defense.gouv.fr/amiad

AI Safety Directory. (2026, 25 mars). *Attaques adversariales sur l'IA : le guide complet de l'apprentissage automatique adversarial (2026).* https://aisecurityandsafety.org/fr/guides/adversarial-attacks/

Akkodis. (2025, 14 février). *Edge AI et systèmes embarqués : un atout clé pour la défense.* https://www.akkodis.com/fr/publications/articles/edge-ai-et-systemes-embarques-defense

Amazon Web Services. (s. d.). *Que sont les MLOps ? – Explication des opérations de machine learning.* Consulté le 6 juillet 2026. https://aws.amazon.com/fr/what-is/mlops/

Aschenbrenner, L. (2024). *Situational Awareness: The Decade Ahead*. Situational Awareness. Source utilisée pour la dépendance calcul, énergie, GPU, data centers et montée en puissance des clusters d'entraînement IA.

Athalye, A., Engstrom, L., Ilyas, A., & Kwok, K. (2017, 31 octobre). *Fooling neural networks in the physical world with 3D adversarial objects*. labsix. https://www.labsix.org/physical-objects-that-fool-neural-nets/

Boero, A. (2026, 4 juillet). *La DGA mise sur Greenerwave et Eutelsat pour mieux connecter les armées françaises depuis l'espace*. Clubic. https://www.clubic.com/actualite-619960-la-dga-mise-sur-greenerwave-et-eutelsat-pour-mieux-connecter-les-armees-francaises-depuis-l-espace.html

Boutin, B., Woodcock, T. K., & Soltanzadeh, S. (Eds.). (2026). *Legal, Ethical, and Technical Dilemmas in Military Artificial Intelligence*. T.M.C. Asser Press / Springer. Source utilisée pour les limites juridiques, éthiques et techniques de la délégation de raisonnement militaire à l'IA, ainsi que les capacités cyber autonomes.

CEA. (2023, 24 mai). *Une interface cerveau-machine (BCI) permet à une personne paraplégique de contrôler sa marche par la pensée.* https://www.cea.fr/presse/Documents/actualites/CP_Pont-digital-Gert-Jan-NATURE.pdf

Centre de doctrine et d'enseignement du commandement. (2023). *Cahiers de la pensée militaire*. https://www.penserleson.fr/cdec

Claude de Ganay et Fabien Gouttefarde. (2020, 22 juillet). *Rapport d'information de la Commission de la défense nationale et des forces armées sur les systèmes d'armes létaux autonomes (SALA)* (n° 3248). Assemblée nationale.

Comandré, M., & Mevellec, M. (2024, 17 décembre). *Les défis éthiques et les risques de l'intelligence artificielle militaire*. Institut National des Affaires Stratégiques. https://inas-france.fr/ia-militaire-defis-ethiques-intelligence-artificielle/

Comité d'éthique de la défense. (2021). *Avis sur l'autonomie dans les systèmes d'armes létaux.* https://www.defense.gouv.fr/ministere/politique-defense/comite-dethique-defense/les-avis-rendus

Comité d'éthique de la défense (COMEDEF). (2025, 14 janvier). *Avis sur l'usage de technologies d'intelligence artificielle par les forces armées*. Ministère des Armées. https://www.defense.gouv.fr/sites/default/files/ministere-armees/20250114_np_comedef_avis-sur-l'usage-des-technologies-d'intelligence-artificielle-par-les-forces-armees.pdf

Commission européenne. (2025). *NEUROQUAD : Disruptive "NEURO-QUantum-AI technology symbiosis" for real-time cognitive monitoring and decision support to improve pilot control and safety.* https://defence-industry-space.ec.europa.eu/document/download/08cc3dee-a4a1-48de-80d4-cd97f122babe_en?filename=FACTSHEET_EDF_2024_LS_RA_DIS_NT_101224494_NEUROQUAD.pdf

Commission européenne. (2026, 27 mars). *From human capital to intelligence management: Data-driven economy and brain-computer interfaces.* https://cordis.europa.eu/project/id/101221675

Commissariat à l'énergie atomique et aux énergies alternatives [CEA]. (2021, 13 juillet). *IA de confiance, IA embarquée : quels enjeux ?* [Entretien avec François Terrier]. https://www.cea.fr/presse/Pages/actualites-communiques/ntic/enjeux-IA-confiance-embarquee.aspx

DARPA. (s. d.). *Neural Engineering System Design (NESD).* https://www.darpa.mil/research/programs/neural-engineering-system-design

DARPA. (2021, 21 décembre). *DARPA open sources resources to aid evaluation of adversarial AI defenses.* https://www.darpa.mil/news/2021/adversarial-ai-defenses

DARPA. (n.c). *SABER: Securing Artificial Intelligence for Battlefield Effective Robustness.* https://www.darpa.mil/research/programs/saber-securing-artificial-intelligence

DataVLab. (2026, 7 février). *Techniques d'annotation LiDAR pour véhicules autonomes.* https://datavlab.ai/fr/post/techniques-dannotation-pour-le-lidar-et-la-fusion-de-capteurs-dans-les-vehicules-autonomes

Databricks. (2026, 2 juin). *L'IA dans la défense : comment l'intelligence artificielle remodèle la sécurité nationale.* https://www.databricks.com/fr/blog/ai-in-defense-industry

De Ganay, C., & Gouttefarde, F. (2020). *Rapport d'information de la Commission de la défense nationale et des forces armées sur les systèmes d'armes létaux autonomes (SALA)* (Rapport N° 3248). https://www.assemblee-nationale.fr/dyn/15/rapports/cion_def/l15b3248_rapport-information

Defensehere. (2025, 20 février). *EDGE va intégrer les radars MILSAR de Meteksan Defence sur les drones GARMOOSHA.* https://defensehere.com/fr/edge-va-integrer-les-radars-milsar-de-meteksan-defence-sur-les-drones-garmoosha/

Direction générale de l'armement. (2024). *Directives sur l'explicabilité et l'IA embarquée.* https://www.defense.gouv.fr/dga

DRONEDGE-RAPID. (s.d.). *DRONEDGE-RAPID : Edge computing et IA pour les essaims collaboratifs.* https://www.dronedge-rapid.fr/

FlowHunt. (s.d.). *Erreur d'entraînement.* https://www.flowhunt.io/fr/glossaire/training-error/

Forecr.io. (2026, 24 mars). *Edge AI in UAVs: Transforming drone intelligence in real time.* https://www.forecr.io/blogs/embedded-systems/edge-ai-in-uavs-transforming-drone-intelligence-in-real-time

Gallitelli, V. (2025). *Artificial Intelligence-Enabled Military Decision-Making Process: The Forgotten Lessons on the Nature of War*. *Journal of Advanced Military Studies, 16*(2), 99–130. Project Maven, la réduction de la boucle OODA, le risque des métriques et l'analogie avec le body count de McNamara.

Gary, A. (s. d.). *Intelligence artificielle et armées françaises : une technologie du présent à mettre en œuvre immédiatement*. *Revue Défense Nationale*, Cahier « Faire face à la recomposition du monde – Regards du CHEM, 70e session ». https://www.defnat.com/e-RDN/vue-article-cahier.php?carticle=383&cidcahier=1264

Gautier, L. (dir.). (2026). *Révolutions et changements en cours dans les affaires militaires* [Cycle de conférences]. Chaire Grands enjeux stratégiques contemporains, Université Paris 1 Panthéon-Sorbonne. https://chairestrategique.pantheonsorbonne.fr

Gautier, L. (2026, juin). *Révolutions militaires en cours et politiques d'armement*. *Revue Défense Nationale*, (891), 84-96. https://www.defnat.com/e-RDN/vue-article.php?carticle=23970

Gielas, A. M. (2025, 21 août). *Warfare at the speed of thought: Can brain-computer interfaces comply with IHL?* https://blogs.icrc.org/law-and-policy/2025/08/21/warfare-at-the-speed-of-thought-can-brain-computer-interfaces-comply-with-ihl/

Harper, J. (2026, 8 avril). *Army eyeing automated target recognition tech to detect explosive hazards, battlefield obstacles.* https://defensescoop.com/2026/04/08/army-automated-target-recognition-breaching-operations/

Hern, A. (2017, 3 novembre). *Shotgun shell: Google's AI thinks this turtle is a rifle*. *The Guardian*. https://www.theguardian.com/technology/2017/nov/03/googles-ai-turtle-rifle-mit-research-artificial-intelligence

IBM. (2025, 9 mai). *Qu'est-ce que le LiDAR ?* https://www.ibm.com/fr-fr/think/topics/lidar

Institut des hautes études de défense nationale (IHEDN). (2025, 3 septembre). *Souveraineté numérique : l'autre front des armées françaises.* https://ihedn.fr/notre-selection/souverainete-numerique-lautre-front-des-armees-francaises/

Intelligence Artificielle. (2026, juin). *Accès aux modèles, contrôle export et souveraineté IA : les nouvelles dépendances de l'intelligence artificielle.* https://intelligenceartificielle.com/notes/acces-modeles-controle-export-souverainete-ia/

Kuntz, C. (2025). *Artificial Intelligence and War: How the Department of Defense Can Lead Responsibly*. CSIS Strategic Technologies Program. Source consultée en appui sur la gouvernance IA militaire américaine, mais moins mobilisée dans la dernière version du texte.

Lagneau, L. (2026, 27 janvier). *L'armée de Terre continue d'évaluer son nouveau système de communication hybride « HYDRE »*. *Zone Militaire*. https://www.opex360.com/2026/01/27/larmee-de-terre-continue-devaluer-son-nouveau-systeme-de-communication-hybride-hydre/

La Tribune. (2025, 23 octobre). *Aéronautique : Zero Industries permet aux drones de voler sans GPS.* https://www.latribune.fr/article/defense-aerospatiale/40270435201470/aeronautique-zero-industries-permet-aux-drones-de-voler-sans-gps

Le Grand Continent. (2026, 2 juillet). *Plus de 90 % des modèles d'IA les plus utilisés dans le monde sont américains ou chinois*. Source utilisée pour le chiffre clé : 47 des 50 modèles les plus utilisés sont américains ou chinois, et la France reste présente via Mistral AI/NeMo.

Lockself. (2025, 29 octobre). *Porte dérobée (backdoor) : comprendre, détecter et bloquer la menace.* https://www.lockself.com/blog/porte-derobee-backdoor-detection-protection

Loi n° 2023-703 du 1er août 2023 de programmation militaire relative aux armées (LPM) pour les années 2024 à 2030. (2023). *Journal officiel de la République française*. https://www.legifrance.gouv.fr/jorf/id/JORFTEXT000047914986

Luo, C. (2026). *Using LiDAR output to identify atmospheric rotors: A convolutional neural network approach*. *Meteorological Applications, 33*(2), e70187. https://doi.org/10.1002/met.70187

Martre, H. (Prés.). (1994). *Intelligence économique et stratégie des entreprises*. Commissariat général du Plan, La Documentation française. Source utilisée pour l'ancrage "Harbulot / intelligence économique" : gestion stratégique de l'information, rapports de force entre nations, rôle de l'État et mobilisation public-privé.

Mazzucchi, N., Lassalle, B., & Mourtont, J. J. (2018, 9 janvier). *Observatoire de l'armée de Terre 2035 Année 2 - Note n°2 : Impacts de l'intelligence artificielle dans le champ de bataille sur les fonctions de supériorité opérationnelles de l'armée de Terre à l'horizon 2035*. Fondation pour la Recherche Stratégique. https://www.frstrategie.org/web/documents/programmes/observatoire-armee-de-terre-2035/publications/2018/22.pdf

Ministère des Armées. (2024, 14 novembre). *IA de Défense : le défi de la souveraineté.* https://www.defense.gouv.fr/actualites/ia-defense-defi-souverainete

Ministère des Armées et des Anciens combattants. (2021, 20 octobre). *Lancement de l'appel à projets annuel de recherche auprès des 4 écoles sous tutelle de la DGA.* https://www.defense.gouv.fr/aid/actualites/lancement-lappel-a-projets-annuel-recherche-aupres-4-ecoles-tutelle-dga

Ministère des Armées et des Anciens combattants. (2022, 1 mars). *Le programme Scorpion.* https://www.defense.gouv.fr/dga/programme-scorpion

Ministère des Armées et des Anciens combattants. (2022, 26 octobre). *Le Fonds innovation défense investit dans Outsight, fleuron français du domaine de l'intelligence spatiale 3D.* https://www.defense.gouv.fr/aid/actualites/fonds-innovation-defense-investit-outsight-fleuron-francais-du-domaine-lintelligence-spatiale-3d

Ministère des Armées et des Anciens combattants. (2025, 1 septembre). *Données et IA.* https://www.defense.gouv.fr/cnd/nos-missions/enjeux-du-commissariat-au-numerique-defense/donnees-ia

Ministère des Armées et des Anciens combattants, Task Force IA. (2019, septembre). *L'intelligence artificielle au service de la défense* (Rapport). https://www.vie-publique.fr/files/rapport/pdf/270333.pdf

MIT CSAIL. (2024). *Class imbalance, outliers, and distribution shift*. *Introduction to Data-Centric AI*. https://dcai.csail.mit.edu/2024/imbalance-outliers-shift/

MIT News. (2018, 16 novembre). *I think, therefore I code.* https://news.mit.edu/2018/student-jessy-lin-computer-science-philosophy-1116

Nazar, A. M., Celik, A., Selim, M. Y., Abdallah, A., Qiao, D., & Eltawil, A. M. (2026). *ENWAR: A RAG-Empowered Multi-Modal LLM Framework for Wireless Environment Perception*. *IEEE Communications Magazine*. Source utilisée pour les capteurs multimodaux, la fusion GPS/LiDAR/caméra, la perception environnementale et la vulnérabilité de la chaîne perception-décision-action.

Organisation des Nations Unies. (2023). *Rapport sur les systèmes d'armes létaux autonomes.* https://www.un.org/disarmament/fr/

OTAN. (2024, 10 juillet). *Summary of NATO's revised Artificial Intelligence (AI) strategy.* https://www.nato.int/en/about-us/official-texts-and-resources/official-texts/2024/07/10/summary-of-natos-revised-artificial-intelligence-ai-strategy

Red Hat. (s. d.). *Le MLOps, qu'est-ce que c'est ?* Consulté le 6 juillet 2026. https://www.redhat.com/fr/topics/ai/what-is-mlops

Royaume du Maroc. (2025). *Contribution sous le thème : « Application de l'Intelligence Artificielle dans le Domaine Militaire : Opportunités et Défis (Hors SALA) dans un contexte de paix et de sécurité internationale »*. Assemblée générale des Nations Unies, Première Commission. https://docs-library.unoda.org/General_Assembly_First_Committee_-Eightieth_session_(2025)/79-239-Morocco-FR.pdf

Safran Electronics & Defense. (2026, 23 février). *EDGE Group et Safran concluent une alliance stratégique dans les systèmes d'armement intelligents.* https://www.safran-group.com/fr/espace-presse/edge-group-safran-concluent-alliance-strategique-systemes-armement-intelligents-2026-02-23

Secrétariat général de la défense et de la sécurité nationale [SGDSN]. (2026, 29 janvier). *Stratégie nationale de cybersécurité (SNC) 2026-2030*. https://www.sgdsn.gouv.fr/files/files/Publications/20260129_SNC-FR.pdf

SentinelOne. (2026, 28 avril). *Qu'est-ce qu'une attaque adversariale ? Menaces et défenses.* https://www.sentinelone.com/fr/cybersecurity-101/cybersecurity/adversarial-attacks/

Service de santé des armées. (2022). *Rapport d'activité et d'évaluation des traumatismes psychologiques opérationnels.* https://www.defense.gouv.fr/sante

Simpson, S. (2026, 16 janvier). *Military Synthetic Aperture Radar (SAR).* https://www.defenseadvancement.com/suppliers/synthetic-aperture-radar-sar/

Solomon, N. (2026). *Regulating LLMs in Warfare*. Stanford University. Source utilisée pour les risques des LLM militaires : escalade, data poisoning, prompt injection, fuite de données sensibles, auditabilité, responsabilité humaine et gouvernance.

Task Force IA. (2021). *Doctrine d'emploi de l'intelligence artificielle de défense.* https://www.defense.gouv.fr/ministere/dossiers/strategie-ia-defense

Thales Group. (s.d.). *BlueScan : Thales révolutionne la lutte anti-sous-marine collaborative.* https://www.thalesgroup.com/fr/actualites-du-groupe/communiques-de-presse/thales-revolutionne-la-lutte-sous-marine-avec-le-nouveau

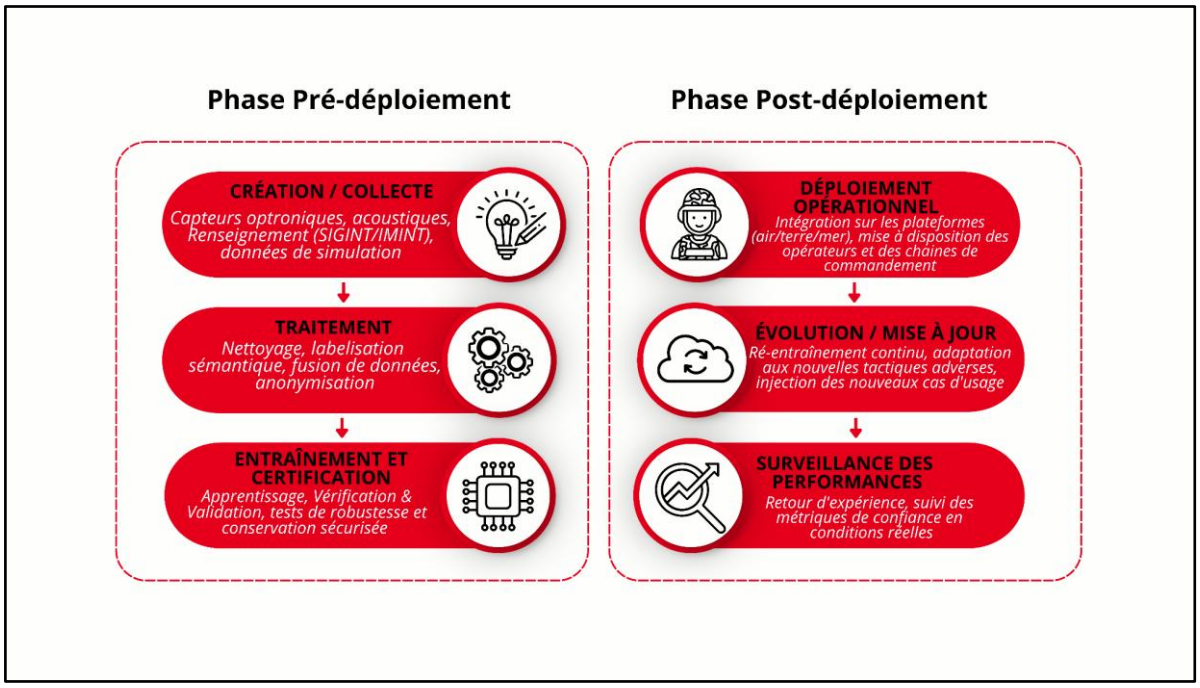
UNODA. (2025, 17 septembre). *Key takeaways of the Military AI, Peace & Security Dialogues 2025.* https://disarmament.unoda.org/en/updates/key-takeaways-military-ai-peace-security-dialogues-2025

Vahle, M. W. (2020, juillet). *Opportunities and implications of brain-computer interface technology.* https://www.airuniversity.af.edu/Portals/10/AUPress/Papers/WF_0075_VAHLE_OPPORTUNITIES_AND_IMPLICATIONS_OF_BRAIN_COMPUTER_INTERFACE_TECHNOLOGY.PDF

Xu, R., Li, X., Chen, S., & Xu, W. (2025). *Nuclear Deployed: Analyzing Catastrophic Risks in Decision-Making of Autonomous LLM Agents*. *Findings of the Association for Computational Linguistics: ACL 2025*, 1226–1310. Source utilisée pour le risque d'agents LLM autonomes en contexte critique et l'idée que de meilleures capacités de raisonnement ne garantissent pas davantage de sûreté.

VI.Annexes

Annexe 1: Infographie cycle de vie de la donnée



Annexe 2: Définition des termes du sujet

- **Edge computing :** technologie qui permet à un appareil de traiter de l'information de manière décentralisée, sans avoir à être connecté à un centre de calcul ou de données. Les modules Edge équipent donc des appareils pouvant fonctionner sans être contrôlés par un opérateur.
- **Attaques adversariales :** Techniques consistant à introduire des perturbations infimes et souvent imperceptibles dans les données d'entrée d'un modèle d'apprentissage automatique, dans le but de le tromper et de provoquer des erreurs de prédiction. Ces manipulations exploitent les faiblesses intrinsèques des algorithmes et constituent une menace sérieuse pour la fiabilité des systèmes d'IA en environnement hostile.

- **Autonomie décisionnelle** : Elle se définit comme « l'aptitude d'un système informatique à interpréter son environnement et à choisir une ligne d'action parmi plusieurs options possibles, sans intervention humaine directe » (Comité d'éthique de la défense, 2021).

- **Défense cybernétique sur le champ de bataille:** Ensemble des contre-mesures déployées pour protéger les systèmes d'information des forces engagées en zone de combat. Elle consiste à détecter et neutraliser rapidement les intrusions, brouillages ou leurres numériques afin de préserver la fiabilité des transmissions et du guidage en temps réel.

- ***Distribution shift*** **:** Modification des propriétés statistiques des données d'entrée auxquelles un modèle d'apprentissage est confronté en opération, par rapport à celles utilisées lors de son entraînement. Cette divergence entraîne une baisse de performance et une perte de fiabilité, car le modèle est testé dans des conditions non prévues initialement.

- **Fusion de capteurs :** Processus consistant à combiner et à corréler les données provenant de multiples capteurs (radar, optique, infrarouge, acoustique, *etc.*) pour obtenir une représentation plus complète et précise de l'environnement. Elle permet de réduire les incertitudes et les angles morts en tirant parti de la complémentarité des sources, améliorant ainsi la qualité de l'information disponible pour la prise de décision.

- ***Human in the loop*** **:** Mode de fonctionnement dans lequel une personne intervient directement à chaque étape critique du processus décisionnel automatisé. Elle valide ou invalide les propositions du système avant leur exécution, garantissant ainsi un contrôle humain sur chaque action entreprise.

- ***Human on the loop*** **:** Mode de supervision dans lequel le système agit de manière autonome mais reste placé sous la surveillance constante d'un opérateur. Celui-ci peut à tout moment interrompre ou modifier le cours des actions, sans toutefois intervenir dans chaque décision élémentaire.

- ***Human out of the loop*** **:** Mode de fonctionnement où l'être humain est totalement absent du cycle décisionnel, le système agissant en pleine autonomie. Aucune intervention ni validation humaine n'est requise en temps réel, la responsabilité étant entièrement déléguée à l'algorithme.

- **IA de décision :** Système d'intelligence artificielle conçu pour analyser des données complexes et proposer ou prendre des choix opérationnels en fonction d'objectifs prédéfinis. Elle ne se limite pas à la perception ou à la classification, mais intègre des processus de raisonnement, d'optimisation et d'évaluation des risques pour orienter une action ou une stratégie.

- **IA Embarquée :** Système d'intelligence artificielle intégré physiquement à un équipement ou un véhicule (drone, blindé, système de guidage) et exécutant ses traitements en local, sans dépendre d'une liaison avec des serveurs distants. Cette architecture permet une réactivité immédiate, une autonomie décisionnelle sur le terrain et une résilience renforcée face aux coupures ou au brouillage.

- ***Machine Learning Operations*** **:** Automatisation de l'ensemble du cycle de vie des modèles d'apprentissage automatique, depuis leur entraînement jusqu'à leur déploiement et leur suivi en conditions réelles. Cela vise à garantir la fiabilité, la reproductibilité et la mise à jour continue de ces modèles au sein d'environnements opérationnels contraints.

- **Sécurité en périphérie tactique (*tactical edge security*) :** Protection des équipements numériques (terminaux, capteurs, drones) déployés sur le terrain, hors des infrastructures fixes et sécurisées. Elle vise à garantir la confidentialité et l'intégrité des données malgré des connexions réseau instables et une puissance de calcul réduite.

- **Vision par ordinateur (*computer vision*) :** Domaine de l'intelligence artificielle qui confère aux machines la capacité d'extraire, d'analyser et d'interpréter des informations significatives à partir d'images numériques ou de flux vidéo. Elle comprend des tâches telles que la détection, la reconnaissance, le suivi d'objets et la reconstruction tridimensionnelle de scènes.

Annexe 3 : Principe de l'attaque adversariale

Image originale

Attaque adversariale : image manipulée pour être interprétée comme un fusil.

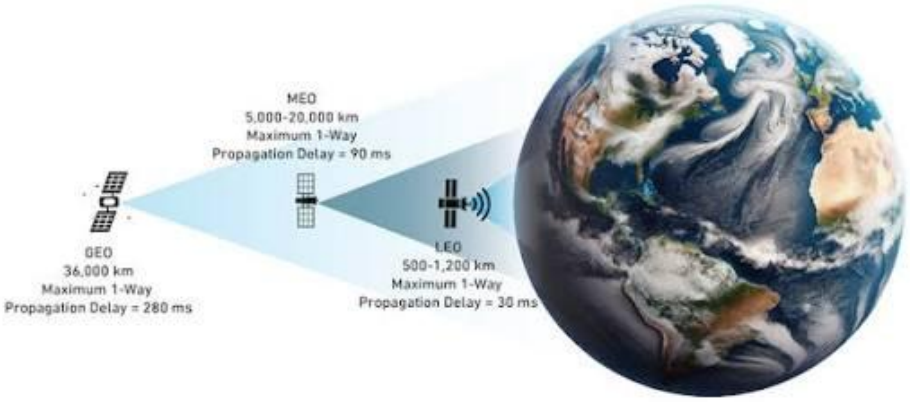
Annexe 4: classification de l'autonomie des systèmes

Cette autonomie des systèmes n'est pas un bloc uniforme, elle s'échelonne du niveau L0 (téléopération complète) au niveau L5 (autonomie totale où la machine choisit sa cible et fait feu seule). Entre ces deux extrêmes se déploient la semi-autonomie de navigation (L2), l'autonomie collaborative en essaim (L3) et la haute autonomie sous tutelle humaine (L4). Face à cette échelle technique, la France fixe une ligne rouge juridique indépassable. En conformité avec l'article 15 de la Constitution du 4 octobre 1958, qui consacre le Président de la République comme le chef des armées et le garant de l'emploi de la force, la doctrine française refuse catégoriquement le niveau L5, qualifié de **Système d'Arme Létal Autonome (SALA)**, c'est-à-dire « un système d'armes capable de sélectionner et d'engager des cibles avec une force létale sans aucune supervision humaine significative » (ONU, 2023). Comme l'a réaffirmé le Comité d'éthique de la défense (2021), la France autorise la robotisation autonome jusqu'au niveau L4 pour les fonctions non-létales (renseignement, logistique, évitement d'obstacles) mais sanctuarise le contrôle humain direct pour chaque ouverture du feu.

Niveaux d'automatisation du système	L0 Système armé pleinement téléopéré	L1 Système armé dupliquant automatique-ment l'action de l'opérateur	L2 Système semi-autonome en déplacement et en détection de cibles	L3 Système armé autonome soumis à autorisation de tir	L4 Système armé autonome sous tutelle humaine	L5 Système armé sans tutelle humaine
Opérateur humain associé au système	L'opérateur humain téléopère à distance le système à l'aide d'une interface de pilotage déportée	L'opérateur humain est augmenté par un système qui l'assiste en dupliquant automatique-ment ses actions	L'opérateur humain supervise le système en lui fournissant un plan de route et des indications de cibles	L'opérateur humain n'intervient que pour donner l'autorisa-tion d'ouvrir le feu sur une cible proposée par le système	L'opérateur humain peut désactiver et reprendre le contrôle du système pleinement autonome	L'opérateur humain n'a pas la possibilité de reprendre le contrôle du système pleinement autonome
Composante mobile-traction du système	Les déplacements du système sont strictement téléopérés par l'opérateur humain	La composante de traction peut suivre et reproduire les déplacements du superviseur humain via ses capteurs	Le système choisit le meilleur chemin en fonction des indications de localisation fournies par l'opérateur	Les déplacements sont décidés par le système en fonction de sa perception du terrain et de ses objectifs de mission	Les déplace-ments sont décidés par le système en fonction de sa perception du terrain et de ses objectifs de mission	Les déplace-ments sont décidés par le système en fonction de sa perception du terrain et de ses objectifs de mission
Composante de détection du système	Les détecteurs du système renvoient des informations à l'opérateur	Les capteurs du système détectent les objets que l'opérateur a détecté	Les capteurs du système détectent automatique-ment les objets cibles potentielles	Les capteurs détectent et reconnais-sent les objets de manière autonome	Les capteurs détectent et reconnais-sent les objets de manière autonome	Les capteurs détectent et reconnais-sent les objets de manière autonome

Tableau des niveaux d'autonomie

Annexe 5: la constellation OneWeb



Satellite LEO, lancé entre 500 et 1.200km de la terre, activité principale de l'entreprise européenne Eutelsat, propriétaire de la constellation OneWeb.

Annexe 6 : Mindmap