MINISTÈRE DES ARMÉES
Liberté
Égalité
Fraternité

COMMANDEMENT DU COMBAT FUTUR

ÉTUDE

Émetteur : Centre d'études stratégiques Terre (CEST) /
Bureau Observatoire des Conflits futurs

25/03/2025

Démythifier l'Intelligence Artificielle

Ce document ne constitue pas une position officielle de l'armée de Terre

Résumé

L'intelligence artificielle (IA), souvent perçue comme l'apanage d'une puissance quasi divine, suscite fascination et crainte en même temps. Pourtant, derrière l'attrait des images futuristes et des récits apocalyptiques se cache une réalité plus sobre : l'IA est une construction humaine, un ensemble d'algorithmes élaborés en imitant certains aspects du raisonnement, mais loin d'atteindre à ce stade une intelligence comparable à celle de l'homme. Démythifier l'IA, c'est alors casser l'illusion d'une machine toute-puissante, en soulignant ses limites intrinsèques et les dangers de sa surestimation. Cette remise en question est d'autant plus essentielle dans un contexte où l'IA est évoquée à tout-va comme la solution universelle aux défis contemporains. Il importe de rappeler que, bien que les systèmes d'intelligence artificielle puissent accomplir des tâches complexes, leur efficacité reste tributaire de la qualité des données d'entraînement et des cadres de régulation qui les encadrent. Loin d'être une entité autonome, l'IA reproduit souvent les biais et les failles de ses créateurs, et son application sans supervision adéquate peut mener à des dérives inattendues.

Mlle Charline Geay, responsable de projet

Clôture du Sommet pour l'Action sur l'IA le 11 février 2025, avec les leaders mondiaux, au Grand Palais à Paris : https://www.telerama.fr/debats-reportages/sommet-de-l-ia-pour-finir-la-france-decide-d-innover-d-abord-et-de-reflechir-ensuite-7024320.php

Sommaire :

Introduction

La traduction du terme « *Artificial Intelligence* » par « intelligence artificielle » n'est pas le fruit d'un hasard. Ce choix, hérité des travaux pionniers de John McCarthy dans les années 1950, traduit fidèlement l'idée d'une intelligence créée artificiellement par l'homme. « Intelligence artificielle » capture l'essence de la démarche : il s'agit d'imiter, à l'aide de mécanismes algorithmiques, certains traits de l'intelligence humaine et non de créer un savoir ou une donnée de manière autonome. Ce travail se veut une invitation à repenser le rapport à l'IA en brisant ses promesses exagérées. En déconstruisant l'image d'une technologie omnipotente, cette étude cherchera à montrer que, pour être bénéfique, l'IA doit être encadrée par des principes éthiques et des régulations rigoureuses, afin de garantir qu'elle serve véritablement l'intérêt général sans renforcer les inégalités ou se substituer à la réflexion humaine lors de la prise de décision.

Titre I : Mieux définir l'intelligence artificielle

La Commission européenne qualifie de « *système d'intelligence artificielle* » un logiciel « *développé au moyen d'une ou plusieurs des techniques et approches* » telles que « *l'apprentissage automatique* » et « *qui peut, pour un ensemble donné d'objectifs définis par l'homme, générer des résultats tels que des contenus, des prédictions, des recommandations ou des décisions influençant les environnements avec lesquels il interagit* »[1]. Cette définition délimite le cadre du sujet, à savoir celui d'un modèle aux contours humains, dont le fonctionnement semble avant tout porter sur l'assistance, bien en deçà du mythe inquiétant d'un remplacement de l'homme par la machine.

1. L'IA, quel périmètre ?

L'intelligence artificielle, loin d'être une réalité homogène, couvre un éventail de techniques et d'applications, dont les contours exigent d'être précisés afin de mieux comprendre son périmètre et ses véritables capacités.

a) L'IA, une vieille histoire

S'attarder sur l'intelligence artificielle, c'est avant tout se pencher sur les contours d'une entité aux multiples facettes, omniprésente dans le champ de la recherche contemporaine. Dans des domaines aussi variés que les services de santé, l'administration, la logistique ou encore la planification des opérations militaires, aucune sphère ne semble désormais à l'abri de l'influence croissante de systèmes numériques sophistiqués, conçus pour anticiper et répondre aux besoins humains. L'intelligence artificielle est invoquée dans tous les secteurs, mais sa définition réelle demeure sujette à débat. Selon le consensus scientifique, il s'agit d'un ensemble de technologies capables d'imiter, au moins partiellement, les fonctions cognitives de l'esprit humain. Cette imitation se traduit par l'automatisation de tâches spécifiques, l'usage du discernement sémantique et la reconnaissance de formes, de motifs, de symboles ou de schémas dans divers domaines, qu'il s'agisse du langage, de l'écriture ou même de l'analyse d'images. L'intelligence artificielle se construit sur des modèles préexistants, enrichis par des bases de données et des concepts approfondis, et s'adapte continuellement aux besoins définis par ses utilisateurs. En somme, ces outils sont malléables et se déclinent selon les finalités que chacun leur attribue, oscillant entre une simple aide à la décision et un partenaire autonome dans la résolution de problèmes complexes.

Pourtant, l'intelligence artificielle telle que définie aujourd'hui n'est pas le fruit d'une découverte soudaine, mais le résultat de plusieurs décennies de recherches assidues et d'innovations progressives dans le domaine algorithmique. Afin de mieux comprendre son évolution, il convient de revenir sur ses balbutiements et d'examiner les premières tentatives d'automatisation de la pensée par la machine. Au XIX^{e} siècle, Charles Babbage conçoit *l'Analytical Engine*, le premier dispositif d'ordinateur programmable, qui marque une étape déterminante dans l'histoire du calcul mécanique. Cette machine, capable d'automatiser des processus par le biais de la programmation, était en mesure d'exécuter des calculs complexes tout en stockant des résultats intermédiaires. La présence d'une « mémoire » préfigurait déjà les systèmes de stockage de données actuels, qui permettent aux algorithmes de puiser dans un vaste réservoir de données et de connaissances. Dans ce contexte, la mathématicienne Ada Lovelace jouera un rôle crucial en rédigeant, en 1843, le tout premier programme informatique destiné à cette machine, établissant ainsi les fondations d'un domaine en perpétuelle expansion[2].

La deuxième étape clé de cette évolution fut marquée par l'intervention d'Alan Turing, considéré comme l'un des pères de l'informatique moderne. Dans son ouvrage *Computing Machinery and Intelligence*, Turing envisage la possibilité d'intégrer une forme de « psyché » humaine dans une machine, posant ainsi les prémices d'une intelligence simulée. Il propose le célèbre test

[1] *Commission européenne, « Proposition de règlement établissant des règles harmonisées sur l'intelligence artificielle (Artificial Intelligence Act) », COM/2021/206 final, 21 avril 2021,* https://eur-lex.europa.eu/legal-content/FR/TXT/?uri=CELEX%3A52021PC0206.

[2] Encyclopædia Britannica, « Analytical Engine », *Encyclopædia Britannica Online*, https://www.britannica.com/technology/Analytical-Engine.

d'imitation, désormais connu sous le nom de « Test de Turing », qui vise à évaluer la capacité d'un ordinateur à se faire passer pour un être humain lors d'un échange de questions-réponses. Ce test, reposant sur l'idée d'une mémoire évolutive et adaptable, ouvre la voie à des systèmes capables d'apprendre de leurs interactions. La terminologie même d'« intelligence artificielle » ne sera popularisée qu'en 1956 lors de *l'Atelier de Dartmouth*, organisé dans une université du New Hampshire. À cette occasion, des chercheurs éminents en sciences cognitives et en informatique, parmi lesquels figuraient John McCarthy, Marvin Minsky et Claude Shannon, se réunissent pour définir les grands principes d'une théorie unifiée, jetant ainsi les bases du *Machine Learning* et des *Neural Networks* tels qu'ils sont connus aujourd'hui[3].

L'enthousiasme généré par ces premières études a ensuite favorisé l'émergence d'expérimentations concrètes qui allaient transformer les théories en applications tangibles. L'un des exemples emblématiques de cette période est le programme *Logic Theorist*, qui adopte une approche heuristique inspirée des axiomes logiques et des règles de déduction formulées par Whitehead et Russell dans leur ouvrage *Principia Mathematica* [4]. En s'appuyant sur des règles empiriques simplifiées et sur un processus de déduction structuré, ce programme parvenait à élaborer des solutions innovantes, dépassant parfois la capacité de raisonnement humain en contournant les limites naturelles du cerveau. Un tournant décisif survint en 1958 avec l'introduction du neurone artificiel par Frank Rosenblatt, connu sous le nom de *Perceptron*. Ce modèle révolutionnaire introduisit la notion d'apprentissage adaptatif, en mimant la connectivité synaptique des neurones biologiques. Capable de traiter des données souvent incomplètes et d'ajuster ses réponses pour atteindre un équilibre optimal entre prédictions et attentes, le *Perceptron* marqua le début d'une nouvelle ère pour l'intelligence artificielle. Les systèmes conçus à partir de ce principe ne se limitaient plus à une simple logique formelle, mais s'enrichissaient progressivement d'un apprentissage par rétroaction, ouvrant la voie aux réseaux multicouches et au fameux *Deep Learning*.

Le concept de *Deep Learning* atteint son apogée dans les années 80 grâce aux travaux de Yann LeCun, qui développa les *Convolutional Neural Networks (CNN),* notamment avec le modèle *LeNet*. Ces réseaux de neurones convolutifs[5] permettent la reconnaissance autonome d'images et constituent une avancée majeure dans le traitement visuel par les machines. La technique de convolution appliquée dans ces réseaux offre une capacité d'analyse hiérarchique des données, transformant l'approche traditionnelle dite « *Top-Down* », qui reposait sur des règles prédéfinies et souvent rigides, en une méthode « *Bottom-Up* » essentiellement nourrie par l'accumulation de données[6]. Cette transition marque une rupture fondamentale avec l'intelligence artificielle symbolique, jusqu'alors dominante, qui peinait à produire des résultats véritablement créatifs et adaptatifs. L'intelligence artificielle actuelle est donc le fruit d'un long processus évolutif, qui a su intégrer et dépasser les limites des approches antérieures ; issue des recherches intensives du XXe siècle, elle incarne aujourd'hui l'aboutissement de décennies d'efforts visant à reproduire, ne serait-ce qu'en partie, les mécanismes de l'intelligence humaine. Entre les premières machines programmables de Babbage et les réseaux de neurones complexes d'aujourd'hui, le chemin parcouru témoigne d'une quête incessante pour comprendre et reproduire les processus cognitifs.

b) L'IA, un modèle algorithmique

Partant de ces grands principes, il convient d'abord de déterminer ce qu'est véritablement l'intelligence artificielle et ce qui, en définitive, la constitue. L'intelligence artificielle, c'est essentiellement l'ensemble d'algorithmes qui en font la force et la fragilité

[3] Stanford Encyclopedia of Philosophy, « *Artificial Intelligence* », *Stanford University*, https://plato.stanford.edu/entries/artificial-intelligence/.
[4] *Principia Mathematica* est une œuvre fondatrice de la logique mathématique, rédigée par Alfred North Whitehead et Bertrand Russell entre 1910 et 1913. Elle vise à établir les mathématiques sur une base purement logique en développant une axiomatisation rigoureuse de l'arithmétique, influençant profondément la philosophie analytique et l'informatique moderne.
[5] Un neurone convolutif est un élément d'un réseau de neurones artificiels utilisé pour analyser des images. Il agit comme un filtre qui repère des formes simples (bords, textures) et les combine progressivement pour reconnaître des objets plus complexes. Cette technique permet aux ordinateurs d'identifier des visages, des lettres ou des paysages à partir d'images, un peu comme le fait un cerveau.
[6] La distinction entre les approches *Bottom-Up* et *Top-Down* en intelligence artificielle réside dans leur mode d'analyse et de conception des systèmes. L'approche *Bottom-Up* repose sur l'apprentissage à partir de données et d'expériences, en laissant émerger des comportements complexes à partir de règles simples (ex. réseaux de neurones). À l'inverse, l'approche *Top-Down* impose des règles prédéfinies et des structures logiques pour guider le raisonnement (ex. systèmes experts).

à la fois. À ce titre, Aurélie Jean, chercheuse et scientifique numéricienne ayant consacré de longues études à ce domaine, préfère parler de « modèle algorithmique »[7]. Ce choix de terminologie traduit l'idée qu'à ce jour, aucune machine ne parvient à reproduire de manière totalement fidèle l'esprit humain. Par exemple, il est fréquent d'affirmer qu'un enfant, même en étant très jeune, reconnaît un chat après en avoir vu un seul, alors qu'un ordinateur, même sophistiqué, doit répéter l'apprentissage sur des séries statistiques importantes pour appréhender les contours de l'objet « chat ». Cela permet de constater ainsi que l'intelligence artificielle ne saurait être envisagée comme une entité autonome ; elle demeure avant tout une construction reposant sur des modèles algorithmiques.

Mais qu'est-ce qu'un algorithme ? En général, il est conçu pour accomplir une tâche précise. Il s'agit d'une séquence d'instructions ordonnées et claires, à l'image d'une formule mathématique, qui vise à résoudre un problème spécifique. Autrement dit, il existe autant d'algorithmes que de tâches pour lesquelles ils ont été conçus. Leur nature et leur mode de fonctionnement varient en fonction des missions à remplir : qu'il s'agisse de résoudre des problèmes, de prendre des décisions ou de trier des informations, chaque algorithme s'adapte à l'objectif qu'on lui assigne. Lorsqu'on évoque l'intelligence artificielle, il faut comprendre qu'elle repose sur une pensée structurée selon des systèmes de tri et des calculs préprogrammés, fondée sur des données soumises à une analyse statistique. Dans ce cadre, les algorithmes assurent plusieurs fonctions essentielles. Tout d'abord, ils traitent et transforment les données en les découpant en entrées codifiées, compréhensibles par la machine, souvent à l'aide d'une fonction d'apprentissage. Ensuite, après avoir intégré et « digéré » ces informations, ils paramètrent et optimisent les résultats. Finalement, une troisième opération combine les données traitées avec les objectifs fixés afin de proposer une prise de décision jugée optimale.

Le *Deep Learning* désigne l'étape la plus récente et aboutie à ce stade de l'évolution de l'intelligence artificielle. Dans son acception la plus large, l'intelligence artificielle regroupe un ensemble d'algorithmes conçus pour reproduire, de manière artificielle, certaines fonctions cérébrales que le cerveau humain exécute quotidiennement. Toutefois, cette reproduction reste limitée à une exécution froide et décomposée en opérations logiques et mathématiques. Parmi les approches populaires figure le « *Machine Learning* », qui englobe l'apprentissage en profondeur et se distingue par sa capacité à générer des sorties plausibles à partir d'un jeu de données, qu'il soit étiqueté ou non. Ce processus combine l'analyse supervisée[8], reposant sur des calculs statistiques tels que la régression linéaire[9], qui établit des corrélations entre variables dépendantes et indépendantes[10]. À partir de ces corrélations, l'algorithme effectue une classification en distinguant différentes catégories et prédit des résultats grâce à des arbres décisionnels et des nœuds de décision. Lorsqu'aucune étiquette n'est disponible, le système identifie des structures cachées au sein des données. Dans certains contextes, l'algorithme adopte également un mode d'apprentissage par renforcement[11]. Ce mode repose sur un environnement structuré autour d'un schéma binaire de punitions et de récompenses, ce qui lui permet d'améliorer ses performances au fil du temps[12].

Par ailleurs, d'autres types d'algorithmes jouent un rôle essentiel dans le champ de l'intelligence artificielle. Le traitement du langage naturel, ou *Natural Language Processing (NLP),* en est un exemple flagrant. Ces algorithmes permettent d'appréhender

[7] Aurélie Jean. (2024, 23 octobre). IA : *Mythes à déconstruire, réalités à saisir - Keynote d'Aurélie Jean* [Vidéo]. YouTube, https://www.youtube.com/watch?v=WSTcrL6ujsY.

[8] Méthode d'apprentissage automatique où un ordinateur est entraîné à reconnaître des modèles à partir d'exemples annotés. Il apprend en comparant ses prédictions aux réponses correctes fournies, comme un élève corrigé par un professeur.

[9] Technique utilisée en intelligence artificielle pour prédire une valeur en traçant une ligne qui relie au mieux des points de données. Plus une donnée est proche de cette ligne, plus la prédiction est précise.

[10] En analyse de données, une variable indépendante est un facteur dont on mesure l'effet, tandis qu'une variable dépendante est celle qui évolue en fonction de la première. Par exemple, en prédisant le prix d'un bien immobilier, la superficie (indépendante) influence directement le prix (dépendante).

[11] Méthode où un algorithme apprend par essais et erreurs en recevant des récompenses pour de bonnes actions et des punitions pour de mauvaises, lui permettant d'optimiser progressivement ses décisions.

[12] Jürgen Schmidhuber, « *Deep learning in neural networks: An overview* », *Neural Networks* 61 (2015) 85–117: https://www.sciencedirect.com/science/article/abs/pii/S0893608014002135.

le phrasé humain en analysant la syntaxe, l'orthographe, la grammaire et la sémantique, jusqu'à contextualiser une conversation afin d'en saisir le ton et les nuances. C'est grâce à eux que le concept de *Generative Pretrained Transformer (GPT)* a pu voir le jour, apportant une avancée considérable dans la compréhension et la génération du langage par la machine. De même, les systèmes de vision par ordinateur regroupent des algorithmes spécialisés dans la reconnaissance et la distinction des motifs et objets dans les images, leur permettant même de les nommer et de les classifier.

L'observation générale qui en découle est que l'intelligence artificielle ne cesse de se développer, tout en étant limitée par la distinction fondamentale entre machine et cerveau biologique. Le cerveau humain assimile et organise naturellement les savoirs qu'il reçoit, tandis que la machine opère uniquement par mimétisme, sans intention propre. Sans algorithme, l'intelligence artificielle ne serait rien, et sans le cerveau humain pour programmer ces algorithmes, elle perdrait toute fonctionnalité et son essence même. En définitive, l'intelligence artificielle reste une construction, un assemblage minutieux de modèles algorithmiques qui, malgré leur sophistication, demeurent dépendants de l'ingéniosité humaine pour évoluer et répondre aux défis posés par un monde en perpétuelle mutation.

c) L'IA, simple facilitateur

Après avoir posé les contours techniques de l'intelligence artificielle, il est essentiel de saisir ses usages actuels. Des systèmes d'assistance professionnelle, conçus pour exécuter des tâches spécifiques, à l'accompagnement quotidien offert par les smartphones et autres appareils connectés, les applications d'intelligence artificielle se multiplient et s'invitent désormais dans la vie courante, que ce soit en milieu urbain ou rural. Cette omniprésence est le corollaire d'un monde hyper connecté et interdépendant, où la mondialisation impose souvent le recours à des outils capables de simplifier et de traiter rapidement d'immenses volumes d'informations. Ce phénomène se traduit par l'essor du « *Big Data* » : d'énormes ensembles de données caractérisés par leur volume, leur variété et leur vélocité sont stockés dans des « *clouds* »[13] intelligents. Grâce à la combinaison de logiciels et d'algorithmes performants, ces systèmes traitent et trient en un temps record des masses de données, accumulant un savoir qui facilite leur exploitation par l'humain.

Depuis 1965, la *loi de Moore* prédit que le nombre de transistors sur un circuit intégré double tous les deux ans, entraînant une croissance exponentielle de la puissance de calcul des ordinateurs. Toutefois, c'est à partir des années 2000 que sont apparues les transformations les plus radicales dans le rapport au numérique des sociétés humaines. L'émergence des dispositifs tels que le *Simon Personal Communicator* d'IBM ou l'*iPhone* d'Apple, témoigne qu'en seulement vingt ans, les fonctionnalités intuitives des machines du quotidien se sont considérablement améliorées. Par ailleurs, l'accélération des échanges et des recherches a été rendue possible par des écosystèmes d'interconnexions en réseaux, comme Internet, qui dynamisent la circulation de l'information. Les capacités de stockage, la rapidité de traitement et l'analyse pointue de données se révèlent ainsi être des atouts majeurs pour le monde professionnel et scientifique, expliquant la pénétration toujours plus grande des technologies d'assistance à l'activité humaine.

L'utilisation de l'intelligence artificielle pour gérer le *Big Data* connaît une expansion fulgurante, notamment dans des domaines qui requièrent le croisement de sources diversifiées pour en extraire des schémas, tendances ou modèles. Le secteur médical, par exemple, a su tirer parti de ces avancées et intègre des solutions intelligentes dans ses recherches et au sein de ses établissements. A titre d'exemple, une étude du *njp Digital Medicine* publiée en avril 2024, met en lumière, grâce à des données chiffrées, la complémentarité entre l'intelligence artificielle et l'expertise clinique dans le diagnostic des cancers de la peau. Sur les 2983 études identifiées initialement, 10 ont été retenues pour une méta-analyse. Pour les cliniciens diagnostiquant sans

[13] Infrastructures de stockage et de traitement de données accessibles via Internet, permettant de gérer de vastes volumes d'informations en temps réel grâce à des serveurs distants.

assistance par intelligence artificielle, la sensibilité combinée[14] était de 74,8 % et la spécificité[15] de 81,5 % dans les diagnostics. Avec l'assistance de l'intelligence artificielle, ces performances s'améliorent significativement, atteignant une sensibilité globale de 81,1 % et une spécificité de 86,1 %.[16] Ces chiffres illustrent non seulement la robustesse des outils d'intelligence artificielle, mais aussi leur capacité à compléter les compétences des cliniciens, y compris chez les professionnels non spécialisés, tels que les non-dermatologues. En outre, l'usage de modèles à effets aléatoires bi variés[17] pour estimer ces indicateurs souligne la rigueur méthodologique de l'analyse croisée, renforçant ainsi la validité des résultats.

De surcroît, l'intelligence artificielle contribue à améliorer la performance éducative en adaptant les plateformes d'apprentissage en ligne. Ces outils offrent aux élèves un accompagnement personnalisé et assurent un suivi constant de leurs performances, permettant ainsi de repérer rapidement les zones de faiblesse et d'ajuster les contenus pédagogiques en conséquence. Dans le domaine administratif, l'emploi de *chatbots*[18] et de systèmes de tri sélectif représente un gain de temps considérable face à l'afflux quotidien d'appels et de demandes. Ces outils d'assistance numérique autonomes hiérarchisent les requêtes, ne transmettant aux conseillers que les demandes les plus urgentes et libérant ainsi des ressources pour traiter les dossiers les plus complexes. L'évolution de la traduction linguistique illustre également les progrès réalisés grâce au traitement du langage naturel (NLP). Les applications de traduction actuelles permettent de communiquer instantanément avec des interlocuteurs étrangers, en reconnaissant non seulement la syntaxe et le vocabulaire, mais aussi les accents et les contextes culturels. L'association du *Machine Learning* et du *Neural Machine Translation (NMT)* permet d'obtenir des traductions d'une grande authenticité. Bien que la richesse des concepts civilisationnels et l'intuition humaine échappent encore à la machine, ces systèmes offrent néanmoins d'excellents premiers jets, facilitant ainsi la communication interculturelle.

2. Déconstruire l'approche menaçante de l'IA

L'intelligence artificielle n'est pas une entité autonome destinée à supplanter l'humain, mais un ensemble de méthodes visant à produire des outils pour amplifier ses capacités, les scénarios de domination des machines n'étant qu'une projection de ses peurs.

a) L'IA, visions apocalyptiques sur le long terme

Dans cette optique, le déploiement massif des intelligences artificielles génératives textuelles, à l'instar de *ChatGPT* rendu accessible à un public non averti dès 2022, a suscité de nombreux débats sur l'éventuel dépassement de l'homme par la machine. Bien que ces scénarios, nourris par l'imagination fertile des auteurs de fiction, séduisent le grand public, ils paraissent pour le moins improbables aux yeux des ingénieurs qui travaillent sur ces technologies depuis de nombreuses années. Dès 2016, Bloomberg s'attelait déjà à concevoir des algorithmes destinés à générer des articles de presse et à assister les journalistes économiques dans la réalisation de travaux d'investigation approfondis. Toutefois, alors que ces outils génératifs étaient initialement conçus à des fins professionnelles et commerciales, leur mise à disposition du grand public n'a pas connu le même équilibre.

Les premières réflexions sur l'accès libre à ces technologies « intelligentes » ont alors fait émerger un ensemble de questions préoccupantes : l'intelligence artificielle remplacera-t-elle l'homme ? Les êtres humains sont-ils voués à devenir obsolètes,

[14] En diagnostic médical, la sensibilité mesure la capacité d'un test à détecter correctement une maladie chez les personnes réellement atteintes. La sensibilité combinée correspond à une moyenne issue de plusieurs études, permettant d'obtenir une estimation plus fiable de cette capacité.
[15] Indicateur qui mesure la capacité d'un test à identifier correctement les personnes non atteintes par une maladie, en évitant les faux positifs. Une spécificité élevée signifie que le test distingue bien les malades des non-malades.
[16] Krakowski, I., Kim, J., Cai, Z.R. *et al.* « *Human-AI interaction in skin cancer diagnosis: a systematic review and meta-analysis". npj Digit. Med.* **7**, 78, (2024). https://doi.org/10.1038/s41746-024-01031-w
[17] Méthodes statistiques utilisées pour analyser simultanément deux variables (comme la sensibilité et la spécificité) en tenant compte des variations entre les différentes études. Cela permet d'obtenir des résultats plus robustes et généralisables.
[18] Un *chatbot* est un programme informatique conçu pour interagir avec des utilisateurs via des conversations en langage naturel, en utilisant des règles prédéfinies ou l'intelligence artificielle pour comprendre et générer des réponses automatisées.

incapables de suivre le rythme effréné des machines ? L'intelligence artificielle chercherait-elle à exterminer l'homme ? Faut-il envisager d'octroyer des droits aux robots si ceux-ci accaparent la majorité des emplois ? Une intelligence artificielle pourrait-elle être dotée de sentiments ? Ces interrogations sensationnalistes tendent à décrédibiliser la discipline et à propager des idées fausses sur un outil dont les mécanismes restent souvent méconnus du grand public. Ce climat de confusion et d'inquiétude ne manque pas d'intéresser les grandes entreprises privées et les acteurs médiatiques, qui se sont emparés de ces discours apocalyptiques pour accroître leurs profits. L'intelligence artificielle, désormais devenue un argument de vente majeur, est évoquée sans cesse dans des discours allant du transhumanisme[19] à l'altruisme technologique[20], témoignant d'une fascination pour la notion de « super intelligence ». Le philosophe Nick Bostrom, par exemple, incarne parfaitement cette vision dans ses écrits, reprenant des thèmes qu'Isaac Asimov avait déjà abordés dans *Les Robots*, publié en 1950[21]. Selon ces courants de pensée, l'intelligence biologique serait progressivement supplantée par des entités artificielles, ouvrant ainsi la voie à un monde dominé par les machines.

Au-delà des récits de fiction et des écrits au ton existentiel, les géants du numérique (Google, Apple, Facebook, Amazon et Microsoft) continuent d'enrichir leur portefeuille en adoptant un narratif de gardiens responsables. Ces entreprises, qui s'adressent à un vaste marché de consommateurs fidèles, exploitent des récits pessimistes pour convaincre les pouvoirs publics d'adopter des lois qui sécurisent leur position de monopole. Ces entreprises prévoient d'investir des sommes colossales dans l'intelligence artificielle en 2025, avec Amazon en tête (100 milliards de dollars), suivi de Microsoft (80 milliards de dollars) et Google (75 milliards de dollars)[22]. Parallèlement, celles-ci acceptent de se plier au jeu de la régulation à la demande de Washington, se positionnant ainsi comme des gardiens éclairés et responsables de la technologie. Cette approche leur permet de façonner le cadre réglementaire à leur avantage tout en renforçant leur image de marque. En combinant des investissements massifs et une participation active à la régulation, ces géants de la *Tech* parviennent à maintenir leur domination sur le marché de l'intelligence artificielle, tout en générant des valorisations boursières impressionnantes. Cette stratégie double d'investissement et de régulation proactive leur assure une position de leaders incontestés dans le domaine de l'intelligence artificielle, renforçant ainsi leur monopole sur l'innovation technologique. Le contrôle du narratif médiatique ne s'exerce pas uniquement par les grandes entreprises ; il est également soutenu par certaines fortunes individuelles. Ainsi, en 2014, Elon Musk avait déjà averti que l'intelligence artificielle constituait une « *menace existentielle* » lors d'un discours prononcé au MIT, évoquant l'image d'un *« démon »* en plein essor. Plus récemment, en mars 2023, il a signé une lettre ouverte appelant à une pause de six mois dans la création de systèmes plus puissants que GPT-4, mettant en garde contre les *« risques profonds pour la société et l'humanité »*[23]. Il est cependant ironique de constater que Tesla, l'entreprise dont Musk est le dirigeant, tire pleinement parti des modèles d'intelligence artificielle pour concevoir et entraîner des voitures autonomes.

[19] Le Trans humanisme trouve ses origines dans les années 1920-1950, avec des penseurs comme Julian Huxley, biologiste et premier directeur général de l'UNESCO, qui a popularisé le terme en 1957. Ce mouvement s'est développé avec les avancées technologiques et l'essor de la philosophie post humaniste.

[20] L'altruisme technologique est un concept plus récent, influencé par des courants comme l'altruisme efficace d'Eliezer Yudkowsky et Nick Bostrom, chercheurs en intelligence artificielle et éthique des technologies, qui ont exploré la manière dont l'innovation peut servir l'humanité.

[21] *Les Robots* est un recueil de nouvelles de science-fiction d'Isaac Asimov, publié en 1950, qui explore les interactions entre humains et robots à travers le prisme des Trois Lois de la Robotique. Ces lois, formulées pour encadrer le comportement des robots, sont : 1) un robot ne peut pas blesser un humain ni, par inaction, permettre qu'un humain soit blessé ; 2) un robot doit obéir aux ordres donnés par un humain, sauf si cela entre en conflit avec la première loi ; 3) un robot doit protéger sa propre existence tant que cela ne contredit pas les deux premières lois.

[22] Courrier International, « Le chiffre du jour : les géants de la tech prévoient un investissement record dans l'IA en 2025 »: https://www.courrierinternational.com/article/le-chiffre-du-jour-les-geants-de-la-tech-prevoient-un-investissement-record-dans-l-ia-en-2025_227476

[23] Le Monde, « *Elon Musk et des centaines d'experts réclament une pause dans le développement de l'IA »,* 29 mars 2023, https://www.lemonde.fr/economie/article/2023/03/29/elon-musk-et-des-centaines-d-experts-reclament-une-pause-dans-le-developpement-de-l-ia_6167461_3234.html.

Les visions dystopiques[24] d'une entité destinée à surpasser son créateur portent en elles un symbolisme puissant, évoquant la promesse d'une toute-puissance quasi divine. À l'instar du mythe de Prométhée[25], porteur du feu sacré, l'intelligence artificielle est souvent perçue comme la nouvelle vague destinée à transcender l'espèce humaine et à transformer radicalement son rapport au monde. Certes, l'usage croissant des algorithmes a déjà modifié les modes de vie et le rapport au savoir, mais il semble peu probable que les fonctions cérébrales s'effondrent sous la pression de cette automatisation. Bien au contraire, l'intelligence artificielle offre la perspective de maximiser et d'enrichir les connaissances, agissant comme un catalyseur de l'intellect humain. Comme le suggérait Henri Bergson dans *L'Évolution créatrice*[26], l'homme transcende la nature et ses propres limites biologiques, précisément parce qu'il ne possède pas d'armes naturelles telles que des dents acérées ou des griffes. L'outil est donc, avant tout, un prolongement de la main, mais de la main qui agit comme ferait une intelligence. En ce sens, l'innovation technique n'est rien d'autre que le prolongement de la personne humaine, un reflet de son adaptabilité et de sa capacité à se réinventer. Pour l'intelligence artificielle, il serait plus juste de parler d'une extension moderne, d'une véritable prothèse cognitive. En définitive, bien que les scénarios catastrophistes alimentent l'imaginaire collectif, l'intelligence artificielle apparaît surtout comme un outil puissant, fruit de l'ingéniosité humaine, qui ouvre la voie à de nouvelles formes d'apprentissage et de compréhension.

b) Les limites de l'IA dans le champ cognitif

En se référant aux thèses de George Sternberg, et plus particulièrement à sa *Théorie triarchique de l'intelligence* parue en 1988, il apparaît clairement que le cerveau humain ne se limite pas à des approches purement psychométriques. L'erreur commise par la recherche scientifique, dans ses premières études sur les capacités cognitives, fut de réduire l'intelligence aux seuls résultats obtenus par des tests de quotient intellectuel (QI)[27]. Sternberg, professeur et psychologue de renom, soutient que l'intelligence humaine s'étend bien au-delà des conceptions traditionnelles. Selon lui, l'intelligence se décline en trois dimensions complémentaires : l'intelligence analytique, l'intelligence créative ou expérientielle, et l'intelligence pratique ou contextuelle. La dimension analytique met l'accent sur la capacité à raisonner, à évaluer et à résoudre des problèmes abstraits en s'appuyant sur les mathématiques et la logique, ce qui constitue le socle des tâches académiques. Les processus mentaux impliqués (planification, prise de décision et encodage de l'information) sont aujourd'hui reproduits, dans une large mesure, par l'intelligence artificielle. Cependant, il convient de s'interroger sur les deux autres dimensions. Bien que l'intelligence artificielle soit désormais capable de générer du contenu artistique en croisant des œuvres humaines, elle ne fait que reproduire des motifs sans en saisir l'intention. Luc Julia, créateur de l'assistant vocal *Siri*, refuse de qualifier ces systèmes d'« *IA créatrice* » et préfère parler d'intelligence « *augmentée* », soulignant ainsi que, malgré leur capacité à imiter des formes artistiques, ces machines demeurent incapables de surpasser l'ingéniosité du génie humain.

Ainsi, les premiers théoriciens de l'intelligence artificielle, qui s'appuyaient sur une conception de l'intelligence humaine limitée au savoir analytique, appartiennent désormais au passé. Le troisième volet de cette approche, à savoir l'intelligence de situation, demeure le dernier jalon inatteignable par les machines. Qu'il s'agisse du sentiment amoureux, de l'humour ou d'une simple empathie, l'anthropomorphisme, illustré par l'effet ELIZA[28], attribué aux intelligences artificielles reste incomplet en l'absence

[24] Se dit d'un futur imaginaire marqué par un contrôle oppressif, des inégalités extrêmes ou un effondrement sociétal, souvent en opposition à une utopie.

[25] Le mythe prométhéen, ancré dans la tradition grecque, symbolise l'acte de transgression par lequel Prométhée défie l'ordre divin en offrant le feu aux hommes, leur conférant ainsi la maîtrise du progrès technique et intellectuel. Cette figure incarne l'ambivalence du savoir : à la fois source d'émancipation et de péril, elle illustre les tensions entre la quête de puissance et les conséquences éthiques de l'innovation.

[26] Dans *L'Évolution créatrice* (1907), Henri Bergson développe une philosophie fondée sur l'élan vital, une force créatrice qui anime l'évolution du vivant au-delà des mécanismes strictement déterministes. Il oppose l'intuition, mode de connaissance directe du réel, à l'intelligence, limitée aux cadres abstraits. Son œuvre propose une vision dynamique du temps (*durée*) et de la vie, influençant la pensée sur la liberté, la création et le progrès. Pour Bergson, la capacité technique est au cœur de l'évolution humaine, l'outil étant l'expression matérielle de l'intelligence appliquée.

[27] Sternberg Robert J. *La théorie triarchique de l'intelligence*. In: *L'Orientation scolaire et professionnelle*, volume 23e numéro 1, Mars 1994. Numéro spécial : *Les techniques psychologiques d'évaluation des personnes*. pp. 119-136. https://www.persee.fr/doc/binop_0249-6739_1994_num_23_1_1477

[28] L'effet ELIZA fait référence à la tendance des humains à attribuer des caractéristiques humaines, comme l'intelligence ou l'empathie, à des systèmes informatiques, même lorsque ceux-ci produisent des réponses simples ou préprogrammées. Ce phénomène tire son nom du *chatbot* ELIZA, créé en 1966 par Joseph Weizenbaum au MIT. ELIZA simulait un psychothérapeute en utilisant des techniques de reformulation simples,

d'une âme véritable, capable de ressentir des passions. En effet, l'intelligence artificielle ne crée pas véritablement, elle génère. La création authentique suppose une intention délibérée, des ressorts émotionnels et une profondeur qui lui échappent. Par conséquent, la machine ne maîtrise qu'une infime part de cette intelligence multiple et ne peut exprimer que ce qui relève de sa programmation analytique. Par exemple, un algorithme de reconnaissance faciale peut détecter, dans une vidéo, des signaux faibles et forts d'émotions telles que la peine ou la joie. Toutefois, ce repérage ne constitue pas une preuve de compréhension : il se contente de reproduire des analogies statistiques à partir d'un apprentissage répétitif.

Il est également intéressant de constater comment l'efficacité de l'intelligence artificielle se voit limitée par la complexité du problème auquel elle est confrontée. Certains contextes désordonnés échappent à son analyse, aussi performante soit-elle. La guerre, par exemple, est souvent qualifiée de phénomène chaotique. Clausewitz, dans son ouvrage *De la guerre*, évoquait déjà ce brouillard complexe et imprévisible, où de multiples facteurs interagissent continuellement. Il écrivait : *« Dans la guerre, tout est simple, mais la chose la plus simple est difficile. Ces difficultés s'accumulent et produisent une friction que personne ne peut bien comprendre s'il n'a pas vu la guerre. Nous pouvons comparer cette friction à celle qui empêche une machine de se mouvoir avec la même facilité que la théorie le supposerait. »* Les opérations militaires ne suivent jamais une linéarité parfaite et chaque conflit présente des nuances propres. Tandis que l'art opératif repose sur le raisonnement par abduction[29] du chef militaire pour atteindre un effet final précis, ce que l'on désigne parfois sous le terme *Operational Design*, l'accumulation de données par l'intelligence artificielle se fonde sur une induction statistique[30]. Ainsi, dans des situations soumises à des contingences historiques et contextuelles, la guerre échappe aux théories purement analytiques que les machines tentent de modéliser. En définitive, l'intelligence artificielle ne peut qu'imiter certains aspects de l'intelligence humaine, tout en restant fondamentalement limitée face à la richesse et à la complexité des comportements réels.

comme transformer les déclarations des utilisateurs en questions. Malgré sa simplicité, de nombreux utilisateurs ont développé un attachement émotionnel au programme, croyant qu'il les comprenait réellement. Cet effet met en lumière la facilité avec laquelle les humains peuvent être amenés à anthropomorphiser des technologies, un phénomène particulièrement pertinent dans le contexte actuel de l'IA conversationnelle avancée.

[29] Mode de pensée qui consiste à formuler l'explication la plus plausible à partir d'indices partiels, souvent utilisé en stratégie et en prise de décision face à l'incertitude.

[30] Méthode qui consiste à tirer des conclusions générales à partir d'un grand nombre de données, en identifiant des tendances ou des probabilités plutôt que des certitudes absolues.

Titre II : L'intelligence artificielle au service du domaine militaire, quelles ambitions pour quel état des lieux ?

Si, donc, la guerre demeure un phénomène fondamentalement chaotique, où l'incertitude et l'imprévisibilité limitent l'efficacité d'une intelligence artificielle purement algorithmique, les grandes puissances n'en investissent pas moins massivement dans son intégration aux opérations militaires. Entre ambition technologique et contraintes opérationnelles, l'intelligence artificielle s'impose progressivement dans les processus de commandement, de renseignement et de combat, transformant en profondeur l'art opératif contemporain. Les États-Unis et la Chine se livrent une véritable course à l'armement algorithmique, chacun développant des stratégies de guerre « *intelligentisée* ». Parallèlement, les conflits actuels, notamment en Ukraine et au Moyen-Orient, servent de véritables laboratoires d'expérimentation pour les systèmes autonomes et les outils d'aide à la décision. Cette transformation militaire s'inscrit dans une continuité historique : comme l'a démontré Freedberg, chaque révolution technologique, de la poudre à canon aux satellites espions, a remodelé la conduite de la guerre et l'intelligence artificielle ne fait pas exception. Toutefois, la réalité du terrain contraste encore avec les ambitions affichées, les armées peinant à passer à l'échelle ces nouvelles capacités, freinées par des défis technologiques, organisationnels et éthiques. Ainsi, où en sont réellement les grandes puissances dans l'intégration de l'intelligence artificielle militaire ? Quels enseignements tirer des conflits récents ?

1. Oppositions et intérêts de puissance

Dans le domaine des intelligences artificielles militaires, la rivalité Etats-Unis/Chine se joue à l'intersection cruciale de la recherche publique, des investissements budgétaires et de l'innovation privée. Maintenir l'initiative requiert de transformer les avancées en prototypes opérationnels, où la synergie entre secteur public et privé est essentielle. Ce constat souligne que la domination technologique ne se construit qu'en réunissant recherche et développement de pointe, ainsi que des ressources budgétaires conséquentes. Cette assemblage justifie l'hégémonie des deux plus grosses puissances économiques mondiales, dans l'innovation numérique, disposant de fonds, d'infrastructures et de main-d'œuvre suffisamment établis pour s'épanouir.

a) Chine et Etats-Unis, les géants de l'IA

La combinaison des domaines militaire et informatique n'est pas une révolution inédite. Depuis déjà plusieurs décennies, de nombreux officiers et stratèges de l'art opératif s'efforcent de maîtriser les prémices d'une intelligence analytique artificielle pour affiner leurs prédictions et orienter leurs décisions sur le champ de bataille. La doctrine dite *Third Offset Strategy*, présentée officiellement par le secrétaire de la Défense américain Chuck Hagel lors du *Reagan National Defense Forum* en 2014, vise à compenser les déséquilibres stratégiques par l'exploitation des technologies de pointe[31]. Concrètement, cette stratégie repose sur l'innovation dans des domaines tels que les armes guidées de précision et les capacités *Anti-Access/Area Denial*[32] pour neutraliser les avantages traditionnels de l'ennemi. Elle invite Washington à investir massivement dans des systèmes autonomes et dans la fusion des technologies conventionnelles avec celles de l'intelligence artificielle et de la robotique, afin de maintenir un avantage compétitif face à des adversaires de plus en plus sophistiqués. Si, dès les années 1950, l'école de pensée militaire quantitative[33] incarnée par Robert McNamara[34] s'appuyait sur des indicateurs purement numériques, la notion de « masse »

[31] War on the Rocks, « *A Game Changing Third Offset Strategy* »: https://warontherocks.com/2014/11/a-game-changing-third-offset-strategy/

[32] Les capacités *Anti-Access/Area Denial* (A2/AD) désignent des stratégies et systèmes défensifs visant à empêcher ou limiter la liberté d'action d'une force adverse dans une région donnée. La Chine applique d'ailleurs cette doctrine en mer de Chine méridionale et dans le détroit de Taïwan en déployant des missiles balistiques antinavires (DF-21D, DF-26), des systèmes de défense aérienne (HQ-9), une flotte sous-marine modernisée et des capacités de guerre électronique pour dissuader toute intervention étrangère, notamment américaine.

[33] L'école de pensée quantitative américaine en stratégie militaire repose sur l'application de modèles mathématiques, de statistiques et d'analyses systématiques pour la prise de décision et la planification des opérations. Développée pendant et après la Seconde Guerre mondiale, notamment par la RAND Corporation, elle privilégie une approche rationnelle et calculatoire pour optimiser l'efficacité des forces armées, en s'appuyant sur des outils comme la théorie des jeux, la modélisation opérationnelle et la gestion des ressources stratégiques. Cette école a fortement influencé la doctrine militaire des États-Unis, en particulier pendant la Guerre froide et dans la planification des conflits modernes.

[34] Robert McNamara (1916-2009) fut secrétaire à la Défense des États-Unis de 1961 à 1968 sous les présidences de John F. Kennedy et Lyndon B. Johnson. Architecte de la modernisation du Pentagone, il appliqua des méthodes analytiques issues du management et de l'école de pensée quantitative, influençant la stratégie militaire américaine durant la Guerre du Viêt-Nam.

s'exprime aujourd'hui sous des formes multiples. Les données traitées par l'intelligence artificielle, ainsi que les équipements, véhicules, armes et effectifs déployés, ne garantissent le succès que lorsqu'elles sont associées à une exigence qualitative rigoureuse. Une flotte de chars obsolètes ou une accumulation de données erronées ne saurait constituer une base fiable pour toute prise de décision. La puissance se mesure désormais autant par la qualité que par la quantité, que ce soit dans le domaine matériel ou numérique.

Cette réflexion incite les grandes puissances à prendre le recul nécessaire pour développer des armes autonomes et intelligentes, technologies encore imparfaites, alors que le monde militaire entame la fusion des systèmes conventionnels avec les innovations en IA et en robotique. Dans cette lutte pour le monopole de la puissance, Washington et Pékin se livrent une concurrence acharnée. À titre d'exemple, sur les 54 000 brevets déposés intégrant de l'intelligence artificielle générative entre 2014 et 2023, la Chine en détient près de 38 000, soit environ six fois plus que les États-Unis[35]. En juillet 2017, le Conseil d'État chinois avait déjà dévoilé son plan de développement de la nouvelle génération d'intelligence artificielle, visant à positionner la Chine en leader mondial d'ici 2030, tant pour l'armée que pour le secteur civil. L'année 2025 devait ainsi marquer le deuxième palier de ces ambitions, illustré par le récent scandale *DeepSeek*[36], qui a révélé des failles de sécurité majeures et des manipulations de données dans les systèmes d'intelligence artificielle, intensifiant ainsi la concurrence entre Washington et Pékin pour le leadership technologique. Par ailleurs, le sommet *REIAM*[37], sur l'utilisation responsable de l'intelligence artificielle dans le domaine militaire, tenu les 9 et 10 septembre 2024 à Séoul, a permis d'élaborer une charte éthique et de réaffirmer le principe de l'humain dans la boucle, dans les prises de décision. Sur les 96 États présents, 30, la Chine en tête, se sont opposés à ce document, illustrant la fracture entre les modèles américains et chinois[38]. La poursuite par les États-Unis de restrictions sur les technologies avancées des semi-conducteurs, freinant ainsi le développement par Pékin de puces de pointe essentielles à ses applications militaires, témoigne d'une rivalité bien ancrée.

b) La dépendance au secteur privé

Un rapide regard sur les géants de la *tech*, les BATX (Baidu, Alibaba, Tencent, Xiaomi) et les GAFAM (Google, Amazon, Facebook, Apple, Microsoft), révèle l'ampleur d'un phénomène qui a propulsé ces entreprises au rang de colosses mondiaux. Prévoyant les transformations radicales du paysage de la défense induite par la robotisation et l'intelligence artificielle, le Ministère de la Défense américain a, dès l'été 2018, inauguré une ère de « guerre augmentée ». La création du *Joint Artificial Intelligence Center* (JAIC) a alors accéléré l'intégration de l'intelligence artificielle dans les systèmes militaires. Financé à hauteur de 2,5 milliards de dollars en 2021 pour soutenir la surveillance assistée par l'intelligence artificielle au sein du CENTCOM[39], le JAIC développe également des applications *d'edge computing*[40] via des calculs neuromorphiques[41], afin d'améliorer la robustesse des réseaux de combat sans recourir à un processeur central. Ces projets suivent le concept de la *Defense Advanced Research Projects Agency*

[35] La Tribune, « *La Chine désormais numéro un sur les brevets d'IA générative devant les États-Unis* »: https://www.latribune.fr/technos-medias/informatique/la-chine-desormais-numero-un-sur-les-brevets-d-ia-generative-devant-les-etats-unis-1001375.html

[36] Le scandale *DeepSeek*, révélé en janvier 2025, concerne une IA chinoise accusée de transférer des données utilisateur vers la Chine, de copier illégalement des technologies de l'organisme américain ayant développé l'application d'IA *OpenAI* et d'intégrer une censure pro-gouvernementale. Plusieurs pays, dont les États-Unis et l'Australie, l'ont interdite pour des risques de cybersécurité, tandis qu'une enquête vise l'acquisition illégale de puces Nvidia, en violation des sanctions américaines.

[37] Responsible AI in the Military Domain, (REAIM) : Le Sommet sur l'Intelligence Artificielle et l'Usage Militaire Responsable.

[38] Asia Pacific Foundation of Canada, « La rivalité entre la Chine et les États-Unis marque le »: https://www.asiapacific.ca/fr/publication/la-rivalite-entre-la-chine-et-les-etats-unis-marque-le

[39] Le CENTCOM (*United States Central Command*) est le commandement central des forces armées américaines, responsable des opérations militaires des États-Unis au Moyen-Orient, en Asie centrale et en partie de l'Asie du Sud. Créé en 1983, il coordonne les interventions dans des zones stratégiques comme l'Irak, l'Afghanistan, la Syrie et le Golfe Persique, avec un focus sur la lutte contre le terrorisme, la stabilité régionale et la protection des intérêts américains.

[40] L'*Edge Computing* est un modèle informatique qui traite les données au plus près des sources (capteurs, appareils connectés) plutôt que dans un cloud centralisé. Cette approche réduit la latence, améliore la réactivité et optimise l'utilisation de la bande passante, notamment pour les applications en intelligence artificielle, Internet des objets (IoT) et 5G.

[41] Les calculs neuromorphiques sont une approche informatique qui imite l'architecture et le fonctionnement du cerveau humain, en utilisant des circuits spécialisés (comme les puces neuromorphiques) pour traiter l'information de manière parallèle et économe en énergie. Inspirés par les neurones et synapses biologiques, ces systèmes sont particulièrement adaptés aux applications d'intelligence artificielle, de robotique et de traitement en temps réel.

(DARPA), agence du Pentagone qui a vu le jour en 1958, destinée à financer les recherches technologiques avancées pour la défense aux Etats-Unis, notamment les balbutiements de l'intelligence artificielle et de la robotique. En juin 2022, le *Chief Digital and Artificial Intelligence Office* (CDAO), fruit de la fusion de plusieurs départements, a pris le relais pour fournir aux forces armées des capacités numériques avancées. En collaboration avec l'état-major interarmées, le CDAO expérimente depuis 2023 le *Programme GIDE (Global Information Dominance Experiments),* qui vise à intégrer de manière globale les opérations militaires à l'exploitation des données par l'intelligence artificielle analytique[42]. Dans ce contexte, les États-Unis déploient des solutions de Commandement et Contrôle Interarmées Tous Domaines (CJADC2) appuyées par une couche d'information unifiée, indépendante des fournisseurs et mieux hiérarchisée.

Le DoD[43] n'en est pas à sa première expérimentation en matière d'intelligence artificielle. Depuis avril 2017, le *Projet Maven*, initialement dirigé par le Général John Shanahan dans le cadre de *l'Algorithmic Warfare Cross-Functional Team* (AWCFT), s'est attelé à intégrer le *Machine Learning* dans les systèmes militaires interconnectés[44]. Conçu pour traiter en temps réel les renseignements collectés par divers dispositifs, du drone aux images spatiales, en passant par les *MQ-9 Reaper* et *MQ-1C Grey Eagle* pour des missions de moyenne altitude longue endurance (MALE), le projet permet le transfert immédiat des données via des liaisons satellites (SATCOM) vers les centres de commandement et les unités terrain. Financé principalement par le Pentagone et en partenariat avec des entreprises comme Microsoft et Amazon, qui fournissent des infrastructures cloud de reconnaissance visuelle et d'apprentissage automatique, le *Projet Maven* s'est étendu. De ses débuts consacrés à la lutte contre l'État islamique, il intervient désormais sur l'ensemble des théâtres d'opération américains, facilitant la gestion intelligente de la collecte des données, l'alerte automatisée et le ciblage prédictif. Ce système libère les analystes des tâches chronophages de tri et leur permet de se concentrer sur des décisions stratégiques complexes.

c) Les doctrines d'emploi de l'IA : la Chine face aux Etats-Unis

Les États-Unis adoptent une stratégie multisectorielle et interarmées qui s'articule autour du *Programme JADC2 (Joint all-Domain Command and Control)*, une initiative visant à intégrer de manière optimale les capacités de commandement et de contrôle dans tous les domaines du combat. Dans cette optique, Washington collabore étroitement avec des entreprises privées de renom, telles que Palantir et Anduril, afin de bénéficier de leurs technologies de pointe dans le traitement de l'information et la cyber sécurité. Parallèlement, le gouvernement américain consacre des investissements considérables à la recherche fondamentale pour protéger ses innovations, en imposant notamment des restrictions à l'exportation qui permettent de préserver l'avantage technologique et la propriété intellectuelle des entreprises nationales. Ce modèle repose sur une confiance importante dans le secteur privé, lequel joue un rôle essentiel dans le développement et la mise en œuvre des solutions numériques au sein des forces armées.

À l'inverse, la Chine déploie une stratégie résolument pragmatique et accélérée, fondée sur une fusion étroite entre le secteur militaire et le secteur civil. Pékin mobilise l'ensemble de ses ressources industrielles et technologiques dans le but de rattraper et de surpasser ses concurrents occidentaux. Le programme *Made in China 2025* constitue l'exemple le plus emblématique de cette démarche, en visant à moderniser et à faire progresser dix secteurs stratégiques clés, notamment les technologies de l'information, l'aérospatial, la robotique, la défense, la cyber sécurité, ainsi que la production de matériaux essentiels tels que les terres rares[45]. Cette stratégie est caractérisée par une volonté de transformer rapidement le paysage industriel national, tout en

[42] U.S. Department of Defense, « *DOD Chief Digital and Artificial Intelligence Office Hosts Global Information Dominance* » : https://www.defense.gov/News/Releases/Release/Article/3282376/dod-chief-digital-and-artificial-intelligence-office-hosts-global-information-d/

[43] DoD (Department of Defense) : Le Département de la Défense des États-Unis, responsable de la politique militaire et de la sécurité nationale du pays. Il supervise les forces armées américaines et coordonne les opérations stratégiques et technologiques en matière de défense.

[44] U.S. Department of Defense, « *DOD Announces Project Maven* ». (Publié en avril 2017) : https://www.defense.gov/News/Releases/Release/Article/1024826/dod-announces-project-maven/

[45] NIDS (National Institute for Defense Studies – Japon), « Commentary – PDF » : https://www.nids.mod.go.jp/english/publication/commentary/pdf/commentary105e.pdf

recourant à des méthodes controversées telles que le piratage industriel et l'exploitation agressive de données collectées localement ou dérobées, des pratiques que Pékin considère comme des atouts dans un environnement où les normes éthiques sont moins contraignantes. En juillet 2019, le livre blanc *La Défense nationale de la Chine dans la nouvelle ère,* marquait un tournant majeur en annonçant une évolution de la doctrine militaire chinoise vers une « *guerre intelligente* »[46]. Cette nouvelle vision, qui remplace les anciennes notions « *d'informatisation* » comme mentionné en 2015, met en avant l'intégration poussée de l'intelligence artificielle dans tous les aspects des opérations militaires.

La stratégie chinoise repose sur une doctrine du levier asymétrique qui vise à transformer ses capacités militaires historiquement limitées en un avantage décisif. Pour Pékin, la montée en puissance ne se limite pas à la quantité, mais s'inscrit dans une reconfiguration qualitative des secteurs clés de l'économie numérique, passant de 7,8 à 10 % du PIB, ainsi que dans le développement d'industries stratégiques émergentes, dont la part pourrait atteindre 17 % du PIB, conformément aux grandes orientations du 14e plan quinquennal 2021-2025[47]. Dans ce contexte, des acteurs privés comme Huawei, DJI et Baidu jouent un rôle crucial dans la défense chinoise. Des soupçons persistent quant à la collaboration de Huawei avec des unités spécialisées de surveillance et un centre de la Commission militaire centrale[48], révélant des liens étroits entre ses programmes de sécurité informatique et les besoins de l'Armée Populaire de Libération.[49] De son côté, DJI a fourni des drones et des systèmes *AeroScope* utilisés dans des opérations en Ukraine[50], illustrant l'exploitation concrète de technologies civiles dans des scénarios de conflit, tandis que Baidu, en partenariat étroit avec des entreprises d'État telles que China Electronics Technology Group Corporation, a contribué à la fusion militaire-civile en intégrant des capacités de *cloud computing* à ses recherches en intelligence artificielle.

Récemment, le modèle de langage naturel *Ernie (Enhanced Representation through kNowledge Integration)*, issu de cette synergie, a fait l'objet de tests sur les chaînes de commandement et de contrôle pour prédire les mouvements ennemis et optimiser le positionnement des troupes sur le champ de bataille[51]. Dans la continuité de cette logique, la Chine a amorcé, dès 2011, la transformation de ses forces de drones en créant des brigades spécialisées dédiées à la reconnaissance et à la frappe. Des plateformes telles que les drones MALE *CH-4*, le *Wing Loong-2* et le drone furtif de combat *Hongdu GJ-11,* sont désormais déployées pour recueillir des renseignements et engager les cibles avec une précision redoutable. L'intégration tactique de drones haute altitude longue endurance (HALE), comme le drone *CH-5*, avec des engins hypersoniques de reconnaissance tels que le *WZ-8*, lancés depuis les bombardiers *H-6*, permet de saturer les réseaux de défense adverses en combinant des effets informationnels et cinétiques[52]. Cette combinaison permet de perturber efficacement les systèmes de défense adverses et de créer une confusion quant à l'origine des frappes.

Les exercices récents témoignent de l'évolution rapide de cette doctrine. Par exemple, en mai 2022, la Chine a mis en service le navire autonome *Zhu Hai Yun*, un dispositif de coordination avancé capable de diriger simultanément plus de cinquante drones aériens, marins et sous-marins dans des opérations synchronisées. Ce navire de 88 mètres de long représente un pas décisif vers l'automatisation intégrale des engagements tactiques, en facilitant une réaction rapide et coordonnée face à des menaces

[46] NIDS (National Institute for Defense Studies – Japon), Publication « Security – 05 janvier 2022 » : https://www.nids.mod.go.jp/english/publication/security/pdf/2022/01/05.pdf

[47] Covea Finance, « Principales orientations du 14ème plan quinquennal chinois » : https://particulier.covea-finance.fr/decryptages/le-point-de-vue-de-lexpert/principales-orientations-du-14eme-plan-quinquennal-chinois

[48] La Commission Militaire Centrale (CMC) est l'organe suprême de commandement des forces armées chinoises, contrôlant à la fois l'Armée populaire de libération (APL) et la police armée chinoise. Présidée par le secrétaire général du Parti communiste chinois, elle incarne le lien direct entre le parti et l'armée, assurant la direction stratégique et politique des affaires militaires.

[49] Capital, « *Des employés de Huawei ont collaboré avec l'armée chinoise sur des projets de recherche* » : https://www.capital.fr/entreprises-marches/des-employes-de-huawei-ont-collabore-avec-larmee-chinoise-sur-des-projets-de-recherche-1343156

[50] Le système *AeroScope* de DJI permettait de détecter et d'identifier les drones DJI en temps réel. Utilisé en Ukraine, il aurait été exploité par la Russie pour localiser les opérateurs ukrainiens, soulevant des inquiétudes en matière de sécurité. Face aux controverses, DJI a suspendu ses activités en Russie et en Ukraine, puis a discrètement arrêté la production d'AeroScope en mars 2023.

[51] ZDNet, « Ernie Bot 40 plus fort que ChatGPT : c'est-ce qu'affirment ses créateurs » : https://www.zdnet.fr/actualites/ernie-bot-40-plus-fort-que-chatgpt-c-est-ce-qu-affirment-ses-createurs-39961904.htm

[52] Araya, D., & He, A. (2024). Chinese Military Applications of AI. In United States-China Multilateralism in the Age of Military AI (pp. 8–10). Centre for International Governance Innovation. http://www.jstor.org/stable/resrep65247.12

multiples sur différents théâtres d'opération[53]. Initialement conçu pour de la cartographie et de l'étude océanographique, il va de fait permettre à la Chine d'étendre sa conquête maritime, comme elle revendique des territoires en Mer de Chine Méridionale depuis plusieurs décennies. De surcroît, lors du *Zhuhai Air Show 2024*[54], le drone-mère *JeTank* a été présenté comme une innovation majeure. Capable de transporter une charge utile de près de 6 tonnes, il atteint un poids en vol qui peut monter à 16 tonnes en déplacement pour 25 mètres d'envergure, faisant de ce dispositif l'un des plus gros de sa catégorie dans l'arsenal chinois. Ce véhicule aérien d'attaque et de reconnaissance est fonctionnel, sans pilote, et déplace jusqu'à huit points d'emports externes, notamment pour des bombes, des missiles, voire des drones de petite taille. Il participe ainsi à la flexibilité stratégique par sa capacité de lancement de drones en autonomie au-dessus du champ de bataille. Ces démonstrations concrètes, relayées par des communiqués officiels et des rapports de presse émanant du ministère de la Défense chinois et d'organismes spécialisés en aéronautique, illustrent parfaitement la capacité de la Chine à conjuguer l'innovation technologique avec des applications militaires tactiques de haut niveau.

Public Defense, "First in the World, China Launched Revolutionary Design New Unmanned Ship Zhu Hai Yun", YouTube, 9 juin 2022, https://www.youtube.com/watch?v=66NTdmGFrso&ab_channel=PublicDefense

L'ensemble de ces développements témoigne d'une volonté chinoise affirmée d'atteindre la supériorité technologique dans le domaine de la défense. En investissant massivement dans des technologies de pointe et en intégrant de manière transparente les secteurs civils et militaires, la Chine se positionne pour dominer le champ de bataille numérique et physique. Cette approche, qui repose sur une stratégie à la fois offensive et adaptative, permet à Pékin de transformer ses capacités militaires en un levier puissant d'influence internationale, anticipant ainsi les futures évolutions des conflits à l'ère de l'intelligence artificielle et des systèmes autonomes.

2. Conflits récents : laboratoires à ciel ouvert pour les emplois de l'IA

La course technologique des intelligences artificielles n'est pas le monopole des hyperpuissances, comme le montre l'étude des conflits actuels où les terrains d'expérimentations sont vastes et quasi-illimités pour les belligérants. Dans un schéma du fort au faible, le développement des systèmes d'armes autonomes par l'entremise des algorithmes entrainées sur des jeux de données prédéfinis, constitue un atout majeur dans les combats, bien qu'il s'accompagne d'une multitude de questionnements éthiques

[53] CNN, « China Zhuhai Airshow: New Weapons » : https://edition.cnn.com/2024/11/19/china/china-zhuhai-airshow-new-weapons-intl-hnk/index.html

[54] Le Zhuhai Airshow, officiellement connu sous le nom d'Exposition internationale de l'aviation et de l'aérospatiale de Chine, est un salon aéronautique biennal se tenant à Zhuhai, dans la province du Guangdong, depuis 1996. Cet événement majeur présente des démonstrations d'aéronefs militaires et civils, ainsi que des lanceurs spatiaux, constituant le plus important salon chinois dans ce domaine.

et techniques. Jusqu'où, alors, s'étend le spectre de l'intelligence artificielle dans les opérations militaires contemporaines et à qui profite ses applications ?

a) Israël/Palestine : la Bande de Gaza en ébullition

Depuis le 7 octobre 2023, un survol de la situation à Gaza révèle l'usage d'un arsenal sophistiqué et de moyens de guerre intelligents, notamment par les Forces de Défense israéliennes (FDI). Israël, reconnu comme l'un des leaders mondiaux dans ce domaine, équipe ses troupes avec l'appui de technologies de pointe et d'ingénieurs spécialisés. Au cœur de son renseignement militaire se trouve l'unité d'élite 8200, souvent comparée à la NSA américaine qui, depuis 2012, repère et recrute des talents au sein des lycées via des programmes tels que *Magshimim*[55] et *Gvahim*[56]. Créée dans les années 1930 sous le nom de Shin Mim 2 durant le mandat britannique et continuellement adaptée aux évolutions technologiques et géopolitiques, cette unité a largement contribué à transformer le pays en un véritable pôle d'innovation et de surveillance[57]. Ainsi, Israël présente le taux le plus élevé de *startups* par habitant, nombre de ces entreprises étant fondées par d'anciens agents issus de l'unité 8200. Par ailleurs, depuis 2023, cette même unité est impliquée dans les enquêtes sur les insuffisances du renseignement ayant précédé l'attaque du Hamas, et concentre désormais ses efforts sur la guerre électromagnétique (ROEM) et la cyberguerre. En fusionnant intelligence artificielle et expertise humaine, elle fait usage du *système Gospel*, qui a récemment fait l'objet de vifs commentaires dans les médias occidentaux.

Connu en hébreu sous le nom de *Habsora*, cet algorithme analyse d'importants volumes de données issues des diverses branches du renseignement israélien, alliant interceptions *SIGINT*, imagerie satellite, renseignement humain (*HUMINT*) et données géospatiales (*GEOINT*), pour générer une liste ciblée d'objectifs. Sa mission principale consiste à offrir aux décideurs militaires une présélection rapide de cibles potentielles. Ainsi, lors de l'opération « Glaive de Fer »[58], il aurait permis aux FDI d'identifier jusqu'à 100 cibles par jour, un chiffre nettement supérieur aux capacités d'analyse purement humaines[59]. Toutefois, cette automatisation soulève la question d'une moindre supervision humaine dans le processus décisionnel. Bien que *Gospel* ne commande pas directement les frappes, sa capacité à accélérer et à systématiser l'identification des cibles réduit le temps disponible pour une évaluation critique par les analystes[60].

Ce phénomène est particulièrement visible avec *Lavender*, un autre système d'intelligence artificielle intégré aux opérations de Gaza. Son rôle consiste à attribuer à chaque individu une probabilité d'affiliation à une organisation hostile, via un système de notation sur une échelle de 1 à 100. Ce programme a permis d'identifier jusqu'à 37 000 Gazaouis comme suspects, facilitant ainsi les frappes dites préventives[61]. Cependant, les documents internes aux FDI indiquent que le taux d'erreur de *Lavender* avoisine les 10 %, ce qui signifie que des milliers de personnes ont pu être prises pour cible sur la base de critères erronés. Dans cette logique d'optimisation algorithmique, *Where's Daddy ?* complète ce dispositif en suivant en temps réel les déplacements des individus marqués par *Lavender*[62]. Grâce à l'interconnexion de données issues de la surveillance mobile et des capteurs *SIGINT*,

[55] Le programme *Magshimim* est une initiative israélienne lancée en 2010, visant à former des lycéens aux compétences en cyber sécurité, en particulier ceux issus des zones périphériques, pour les préparer à intégrer les unités technologiques de Tsahal et le secteur high-tech.
[56] *Gvahim* est une organisation à but non lucratif fondée en 2009, dédiée à l'accompagnement des nouveaux immigrants hautement qualifiés en Israël, facilitant leur intégration professionnelle grâce à des programmes de formation, de mentorat et de mise en réseau.
[57] Amicale Nationale des Transmissions Aéroportées, « Unité 8200 : La sentinelle furtive d'Israël », *Amicale Nationale des Transmissions Aéroportées*, 2 avril 2024, https://amicalenationaledestransmissionsaeroportees.fr/2024/04/02/unite-8200-la-sentinelle-furtive-disrael/.
[58] L'opération Glaive de fer est la réponse militaire israélienne déclenchée fin octobre 2023 suite aux attaques du Hamas et visant à neutraliser les infrastructures terroristes dans la bande de Gaza.
[59] Florian Gouthière et Alexandre Horn, « *Comment l'armée israélienne utilise l'intelligence artificielle pour bombarder Gaza* », *Libération*, 2 décembre 2023, https://www.liberation.fr/checknews/comment-larmee-israelienne-utilise-lintelligence-artificielle-pour-bombarder-gaza-20231202_EMALLXEUEJB7HFEZZPM7XXZBMQ/.
[60] Yuval Abraham, Oren Ziv, Meron Rapoport et Areej Hazboun, « '*Lavender*': The AI Machine Directing Israel's Bombing Spree in Gaza », +972 Magazine, 3 avril 2024, https://www.972mag.com/lavender-ai-israeli-army-gaza/.
[61] Laure de Roucy-Rochegonde et Amélie Ferey, « L'IA au cœur de la stratégie israélienne à Gaza », Institut français des relations internationales (IFRI), 26 février 2025, https://www.ifri.org/fr/presse-contenus-repris-sur-le-site/lia-au-coeur-de-la-strategie-israelienne-gaza.
[62] Times for Palestine, « Unit 8200 Role in the Ongoing AI War », *Times for Palestine*, 10 December 2024, https://timesforpalestine.com/unit-8200-role-in-the-ongoing-ai-war/.

ce programme identifie le moment où une cible rentre à son domicile, souvent perçu comme le moment optimal pour une frappe létale. L'objectif, selon les FDI, est de s'assurer que les cibles identifiées soient isolées afin de minimiser les dommages collatéraux. Toutefois, cette approche a conduit à une multiplication des frappes sur des habitations civiles, exposant ainsi les proches des suspects à des risques accrus.

Mais au-delà du ciblage algorithmique, l'intelligence artificielle est également employée comme un outil stratégique de surveillance et de cartographie du terrain. Israël a mis au point *Depth of Wisdom*, un système conçu pour cartographier et analyser en profondeur la bande de Gaza et les infrastructures du mouvement islamiste palestinien. Cette intelligence artificielle fonctionne en agrégeant des images satellites, des données de drones et des capteurs au sol, permettant de dresser un portrait détaillé des tunnels du Hamas, des caches d'armements et des réseaux de commandement adverses. Dans un environnement urbain densément peuplé et marqué par la présence de structures souterraines, il offre donc un avantage stratégique majeur : il facilite la détection des sites cachés et optimise la planification des raids militaires. Le recours à *Depth of Wisdom* est aussi particulièrement notable dans la surveillance des infrastructures du Hezbollah au Liban, où l'armée israélienne cherche à identifier les entrepôts de roquettes et les quartiers généraux dissimulés au sein de zones civiles. Contrairement à Gaza, où les frappes sont fréquentes, Israël privilégie ici une stratégie de renseignement préventif visant à cartographier en détail les capacités offensives de son adversaire en amont d'un potentiel conflit. L'un des principaux enjeux est d'anticiper les attaques de missiles en localisant leurs zones de stockage et leurs itinéraires de transport.

Parallèlement, lors de l'opération « Gardien des Murs »[63], l'armée israélienne a massivement déployé des essaims de drones opérant en autonomie algorithmique via un système de calcul distribué[64], leur permettant de partager des données et d'adapter leurs trajectoires en temps réel sans intervention humaine directe. Ce mode de fonctionnement a optimisé la reconnaissance, l'identification et la neutralisation des cibles, tout en réduisant la charge cognitive des opérateurs. Des systèmes C2 dopés à l'intelligence artificielle, tels que *Drone Guard*, ont amélioré la coordination et l'automatisation des frappes. Appuyée sur des composants de type radar 3D de la famille *ELM-2026*[65] à courte et longue portée, associé notamment à des algorithmes spéciaux de détection et de suivi de drones, *Drone Guard* emploi des capteurs électro-optiques et du brouillage d'attaque électronique dédié pour perturber les vols d'engins ennemis. Cette unité compacte et abordable, permet un rendement efficace en combinant des options de neutralisation dites « *soft kill* » pour du brouillage, et « *hard kill* » pour de la destruction physique, face à des petits drones commerciaux hostiles, de plus en plus employés pour les actions terroristes. La cinquième génération intègre une architecture ouverte avec une large gamme de capteurs hautes performances dont des systèmes électro-optiques, des radars fixes et rotatifs ainsi qu'une antenne à balayage électronique (AESA)[66] en élévation[67].

Toutefois, cette dépendance croissante aux algorithmes a renforcé un biais de sur-confirmation, où les opérateurs, séduits par la rapidité et la précision apparente des intelligences artificielles, valident mécaniquement les recommandations sans réelle analyse critique. Cette course à l'optimisation, visant à maximiser le nombre de cibles éliminées, s'est faite au détriment du principe de

[63] L'opération « Gardiens des Murs » est une offensive militaire israélienne menée du 10 au 21 mai 2021 contre le Hamas et le Mouvement du Jihad Islamique en Palestine (MJIP) dans la bande de Gaza, en réponse à des tirs de roquettes sur Israël et visant à neutraliser les infrastructures terroristes et à affaiblir les capacités offensives des groupes armés.

[64] Architecture informatique où plusieurs ordinateurs ou processeurs collaborent pour exécuter des tâches simultanément. Dans le contexte des essaims de drones, cela permet un partage instantané des données entre appareils, optimisant la coordination et l'adaptation en temps réel sans intervention humaine.

[65] L'ELM-2026 est une famille de radars de défense aérienne à très courte portée développée par Israël Aerospace Industries. Ces radars 3D utilisent la technologie de formation de faisceau numérique (DBF) pour détecter et suivre des cibles aériennes, y compris des drones et des aéronefs à faible signature radar. Il existe plusieurs versions avec des portées allant de 10 à 20 km, adaptées à la protection des infrastructures critiques et à l'intégration dans des systèmes de défense anti-drones.

[66] Technologie radar utilisant un réseau d'antennes capables de diriger leurs faisceaux électromagnétiques sans déplacement mécanique. Dans le système *Drone Guard*, elle permet une détection rapide et précise des drones en adaptant son champ de surveillance aux mouvements des cibles aériennes.

[67] Israel Aerospace Industries (IAI), « ELI-4030 Drone Guard », *Israel Aerospace Industries (IAI)*, 26 janvier 2020, https://www.iai.co.il/p/eli-4030-drone-guard.

proportionnalité du droit international humanitaire, réduisant la distinction entre combattants et civils et augmentant les risques de frappes aveugles.

b) La Guerre Russo-Ukrainienne : un terrain d'essai quasiment « illimité »

Le terrain ukrainien n'est pas en reste, notamment depuis le début du conflit en 2014, où l'industrie de la *Big Tech* s'est vue offrir une opportunité inédite de mettre à profit ses projets de recherche et de développement dans une guerre où les limites entre les différents champs de la conflictualité et l'implication de certains acteurs restent floues. Dès juin 2022, le ministre ukrainien de la Transformation numérique, Mykhailo Fedorov, ouvre ainsi la porte aux entreprises américaines spécialisées dans la robotique et l'intelligence artificielle[68] : Starlink pour les connexions satellitaires, Palantir pour la gestion du *Big data* et l'analyse prédictive en matière de ciblage, ou encore Clearview AI, qui utilise la reconnaissance faciale pour l'identification d'ennemis. Rapidement, la capitale ukrainienne elle-même devient un hub technologique où se côtoient *startups* locales et mastodontes étrangers, jusqu'à se voir attribuer le surnom de *Mil-Tech Valley***.** L'Ukraine est ainsi devenue un véritable *« terrain d'entraînement à l'utilisation de l'intelligence artificielle »*, exploitant l'asymétrie technologique pour surprendre l'adversaire[69]. Toutefois, Fedorov reconnaît que le recours massif à ces technologies ne suffit pas à vaincre la Russie : il s'agit d'un atout stratégique à intégrer dans la culture de l'armée plutôt qu'une solution miracle. Le label « *Testé en Ukraine* », très prisé des investisseurs et mis en avant dans les salons de défense, illustre parfaitement la logique de marketing obsessionnel qui anime les entreprises privées développant ces technologies. Ce sceau d'approbation sert de justificatif d'efficience, mais masque les limites sémantiques et les dilemmes éthiques de ces systèmes. Par ailleurs, si l'Ukraine mobilise tous ses moyens pour acquérir une supériorité technologique face à la masse vieillissante des équipements russes, Moscou s'y attèle depuis bien longtemps également.

Depuis le discours emblématique de Vladimir Poutine le 1er septembre 2017, la Russie a multiplié ses efforts pour intégrer l'intelligence artificielle dans le domaine militaire. Le président russe déclarait alors : *« L'intelligence artificielle est l'avenir, non seulement pour la Russie, mais pour toute l'humanité. Cela présente des opportunités colossales, mais aussi des menaces difficiles à prévoir aujourd'hui. Quiconque deviendra le leader dans ce domaine deviendra le dirigeant du monde. »* Cette ambition a été officialisée par l'oukase du 10 octobre 2019, établissant une stratégie nationale de développement de l'intelligence artificielle jusqu'en 2030[70]. Soutenue par la Fondation pour la Recherche Avancée[71], en partenariat avec les institutions académiques et les entreprises publiques et privées, cette stratégie visait à positionner la Russie à la pointe de la robotisation du champ de bataille. Toutefois, l'invasion de l'Ukraine a mis en lumière un décalage flagrant entre les ambitions affichées et la réalité opérationnelle. Si la Russie a largement recours aux drones et aux munitions rôdeuses, déjà testés en Syrie, la majorité des systèmes déployés restent rudimentaires. En août 2022, le chef du département du ministère russe de la Défense en charge du développement de l'intelligence artificielle, Vasily Yelistratov, déclarait que cette technologie était désormais intégrée *« dans toutes les armes, en particulier celles de haute précision »,* et que *« plus les armes sont intelligentes, moins les pertes subies seront grandes. »* Pourtant, les faits sur le terrain révèlent des performances bien inférieures aux attentes, remettant en cause la réalité de ces avancées[72].

[68]Emmanuel Grynszpan, « Mykhailo Fedorov, ministre ukrainien : "La guerre asymétrique consiste à utiliser des technologies auxquelles l'ennemi ne s'attend pas" », *Le Monde*, 10 août 2024, https://www.lemonde.fr/international/article/2024/08/10/mykhailo-fedorov-ministre-ukrainien-la-guerre-asymetrique-consiste-a-utiliser-des-technologies-auxquelles-l-ennemi-ne-s-attend-pas_6275112_3210.html.

[69] Agathe Mahuet, « Armée et IA : l'Ukraine est devenu un laboratoire pour ces nouvelles armes intelligentes qui inquiètent l'ONU », *Franceinfo*, 16 avril 2024, https://www.francetvinfo.fr/replay-radio/le-club-des-correspondants/armee-et-ia-l-ukraine-est-devenu-un-laboratoire-pour-ces-nouvelles-armes-intelligentes-qui-inquietent-l-onu_6453404.html.

[70] Thierry Berthier et Yannick Harrel, « La stratégie russe de développement de l'intelligence artificielle », *The Conversation*, 26 novembre 2019, https://theconversation.com/la-strategie-russe-de-developpement-de-lintelligence-artificielle-127457.

[71]Organisation russe créée en 2012 et inspirée de la DARPA américaine, chargée de financer et de développer des technologies stratégiques, notamment dans le domaine militaire.

[72]Anna Nadibaidze, « La guerre low-tech de la Russie contre l'Ukraine », *Le Rubicon*, 3 mars 2023, https://lerubicon.org/la-guerre-low-tech-de-la-russie-contre-lukraine/.

A titre d'exemple, les annonces de drones aux qualités futuristes dont les technologies se sont avérées limitées se multiplient au lendemain des premiers affrontements en Ukraine. Avant le début du conflit russo-ukrainien, les drones *KUB-BLA*, développés par ZALA Aero, étaient présentés comme des munitions rôdeuses de nouvelle génération, intégrant des capacités avancées d'intelligence artificielle pour la reconnaissance et le ciblage autonomes. En théorie, ces drones devaient identifier visuellement leurs cibles grâce à des algorithmes sophistiqués (AIVI)[73] et fonctionner dans des environnements contestés sans assistance humaine. En pratique, leurs performances se sont révélées bien en deçà des attentes : le système d'intelligence artificielle ne parvient pas à distinguer efficacement cibles civiles et militaires, nécessitant ainsi une supervision constante ou un guidage complémentaire[74]. Dans le même registre, les *Geran-2*, version russe des *Shahed-136* iraniens, ont démontré un taux de réussite de seulement 14 % dans l'atteinte des cibles désignées[75], principalement en raison du brouillage GNSS[76] et de l'efficacité de la défense anti-aérienne ukrainienne.

Pire encore, de nombreux drones ont frappé des infrastructures civiles de manière non intentionnelle, faute d'une navigation robuste et d'un ciblage précis. Bien que des améliorations aient été apportées, notamment avec l'ajout de traceurs GSM et d'une connectivité 4G pour le retour d'informations en temps réel, ces drones restent dépendants d'une trajectoire préprogrammée. Contrairement aux systèmes occidentaux plus avancés, ils ne disposent ni d'algorithmes d'apprentissage automatique ni de vision par ordinateur permettant un ciblage dynamique et adaptatif. Si la promesse de l'intelligence artificielle militaire visait à garantir un ciblage plus sélectif, capable de faire la distinction entre soldats et civils, la réalité montre une approche bien plus quantitative que qualitative. La course aux frappes et aux statistiques semble prendre le pas sur la précision des engagements. Le recours aux technologies dépassés sous couvert d'innovations est fréquent[77]. En parallèle, plusieurs modèles de drones, bien loin de l'image futuriste véhiculée par Moscou, ont été détournés de leur usage initial dès le début du conflit. Les *E95M*, *TU-143* et *TU-141*, conçus entre les années 1970 et 1990, ont été recyclés en leurres pour déclencher les défenses anti-aériennes ukrainiennes[78]. Ces appareils, équipés de moteurs à essence pulsée, témoignent du caractère rudimentaire de nombreuses solutions adoptées par la Russie[79]. Privés du moindre système intelligent, ils illustrent l'écart entre la communication officielle et la réalité technologique sur le terrain. Ainsi, l'intelligence artificielle militaire russe reste davantage un outil de propagande qu'une révolution opérationnelle.

Les avancées en matière de drones et d'intelligence artificielle dans le conflit russo-ukrainien ne traduisent pas une rupture technologique majeure, mais plutôt une amélioration progressive des capacités existantes. Largement médiatisée comme une « guerre des drones », cette confrontation met en lumière l'emploi massif de munitions rôdeuses et de plateformes autonomes, mais aussi les limites inhérentes à ces technologies. Si les belligérants tentent d'exploiter au maximum les capacités de ces systèmes, notamment en intégrant des algorithmes avancés de reconnaissance et de ciblage, la réalité opérationnelle révèle un

[73] L'AIVI (Artificial Intelligence and Vision Intelligence) est une technologie combinant l'intelligence artificielle et le traitement de l'image afin d'analyser, interpréter et automatiser la reconnaissance visuelle dans divers domaines, notamment la défense, la surveillance, la navigation autonome et le ciblage militaire. Elle repose sur des algorithmes d'apprentissage automatique et de vision par ordinateur pour identifier des objets, des mouvements ou des comportements en temps réel, améliorant ainsi la précision et la réactivité des systèmes automatisés.

[74] Gregory C. Allen, « Russia Probably Has Not Used AI-Enabled Weapons in Ukraine—But That Could Change », *Center for Strategic and International Studies (CSIS),* 26 mai 2022, https://www.csis.org/analysis/russia-probably-has-not-used-ai-enabled-weapons-ukraine-could-change.

[75] Fabrice Wolf, « Geran-2 : la défense ukrainienne face à l'adaptation russe », *Meta-Defense*, 28 novembre 2024, https://meta-defense.fr/fi/2024/11/28/geran-2-defense-ukrainne-asaptation-ru/.

[76] GNSS (Global Navigation Satellite System) désigne l'ensemble des systèmes de navigation par satellite, incluant le GPS (États-Unis), GLONASS (Russie), Galileo (Union européenne) et BeiDou (Chine), permettant un positionnement précis en temps réel sur l'ensemble du globe.

[77] Hugo Brogli et Lou Rochambeau, « Intelligence artificielle et drones autonomes : une transformation des stratégies militaires modernes ? », *Portail de l'IE*, 15 janvier 2025, https://www.portail-ie.fr/univers/blockchain-data-et-ia/2025/intelligence-artificielle-et-drones-autonomes-une-transformation-des-strategies-militaires-modernes/.

[78] « Russia Manufactures Wooded Drones for Reconnaissance and Ukraine's Air Defense Distraction », *Defense Express*, 5 mai 2023, https://en.defenceua.com/weapon_and_tech/russia_manufactures_wooded_drones_for_reconnaissance_and_ukraines_air_defense_distraction-6612.html.

[79] « Guerre en Ukraine, les drones gagnent leurs galons », *Cerbair*, 8 octobre 2024, https://www.cerbair.com/articles/guerre-en-ukraine-les-drones-gagnent-leurs-galons.

cadre plus contraint où l'humain reste un maillon essentiel de la prise de décision. Loin des discours sur une automatisation complète du champ de bataille, les drones employés dans le conflit restent principalement des outils d'appui, nécessitant une validation humaine pour leurs actions critiques. La classification sur l'autonomie des drones proposée par Thierry Berthier (voir ci-dessous), allant du niveau L0 (système armé pleinement opéré) à L5 (système armé autonome sans tutelle humaine), permet ainsi de situer le niveau de sophistication de ces systèmes. Qu'ils soient russes ou ukrainiens, aucun drone ne dépasse actuellement le niveau L4 « système armée autonome sous tutelle humaine ». Il est important de préciser que cette classification se distingue du cadre standardisé OTAN, conçu pour catégoriser les systèmes aériens sans pilotes en fonction des leurs poids au décollage, leur altitude et leur portée, assurant ainsi une certification au sein des forces alliées pour l'interopérabilité face à la diversité croissante des drones militaires[80].

[80] La classification *NATO UAV*, établie en septembre 2009, divise les systèmes aériens sans pilote en trois catégories basées sur le poids au décollage (MTOW) : Classe I (<150 kg), incluant micro (<2 kg), mini (2-20 kg) et petits (20-150 kg) UAV pour missions tactiques de courte portée ; Classe II (150-600 kg), UAV tactiques pour opérations à moyenne altitude (jusqu'à 18 000 pieds) et portée (jusqu'à 160 km) ; Classe III (>600 kg), UAV stratégiques MALE (Medium Altitude Long Endurance, jusqu'à 30 000 pieds) et HALE (High Altitude Long Endurance, >30 000 pieds) pour missions longue distance (>200 km).

Les six niveaux d'automatisation des systèmes armés

Niveaux d'automatisation du système	L0 Système armé pleinement téléopéré	L1 Système armé dupliquant automatiquement l'action de l'opérateur	L2 Système armé 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 autonome 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 automatiquement 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'autorisation 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 déplacements sont décidés par le système en fonction de sa perception du terrain et de ses objectifs de mission.	Les déplacements 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 détectés.	Les capteurs du système détectent automatiquement les objets et cibles potentielles.	Les capteurs détectent et reconnaissent les objets de manière autonome.	Les capteurs détectent et reconnaissent les objets de manière autonome.	Les capteurs détectent et reconnaissent les objets de manière autonome.
Composante de reconnaissance et d'acquisition de cibles	La reconnaissance et l'acquisition des cibles sont exclusivement réalisées par l'opérateur humain.	L'acquisition des cibles est identique à celle de l'opérateur humain *via* le système de visée de son arme connecté à celui du système.	Le système suggère des objets comme cibles potentielles à l'opérateur humain qui définit les cibles à prendre en compte.	L'acquisition de cibles s'effectue de manière automatique ou dirigée *via* les capteurs du système et ses capacités de reconnaissance.	L'acquisition de cibles s'effectue de manière automatique *via* les capteurs du système et ses capacités de reconnaissance et d'analyse.	L'acquisition de cibles s'effectue de manière automatique *via* les capteurs du système et ses capacités de reconnaissance et d'analyse.
Composante armée du système	Les commandes de tirs du système sont exclusivement actionnées par l'opérateur humain.	Le système ouvre le feu sur une cible si, et seulement si, l'opérateur ouvre le feu sur cette cible.	Le système ouvre le feu sur la cible après autorisation du superviseur humain.	Le système propose une cible et ouvre le feu après autorisation du superviseur humain.	Le système décide de l'ouverture du feu sur la cible qu'il a sélectionné mais peut être désactivé par son superviseur	Le système décide de l'ouverture du feu sur la cible qu'il a sélectionné sans possibilité de désactivation (sauf destruction)

Source : Thierry Berthier, https://shs.cairn.info/revue-defense-nationale-2019-5-page-74?lang=fr

Par exemple, le drone russe *Lancet*, bien que doté d'un système de reconnaissance avancé, requiert une désignation préalable de la cible. Dans le cas du *Lancet-3*, les échecs ont d'ailleurs été fréquents, notamment à l'occasion de tirs fratricides géolocalisés, suggérant une certaine limite dans le système de guidage de l'appareil qui visait très souvent des leurres ou des cibles fictives[81]. De même, le robot de combat présenté comme autonome, le *Marker*[82], souffre de lacunes en navigation et identification, nécessitant une surveillance constante. Du côté ukrainien, le *Saker Scout*[83] et le *Droid TW 12.7*[84], malgré des fonctionnalités semi-

[81] David Hambling, « Russian Loitering Munition Racks up Kills but Shows Limitations », *Forbes*, 1er décembre 2022, https://www.forbes.com/sites/davidhambling/2022/12/01/russian-loitering-munition-racks-up-kills-but-shows-limitations/?sh=408f3a225d58.

[82] Le *Marker* est un véhicule terrestre sans pilote (UGV) russe, développé par la société Androidnaya Tekhnika en collaboration avec la Fondation pour la recherche avancée (FPI). Conçu pour des missions de reconnaissance et de combat, il est équipé de systèmes d'intelligence artificielle permettant une identification et une neutralisation autonomes des cibles. Le *Marker* peut être armé de mitrailleuses, de lance-grenades automatiques et de missiles antichars *Kornet*. Il a été déployé expérimentalement en Ukraine depuis février 2023.

[83] *Saker Scout* est un drone de reconnaissance ukrainien équipé d'intelligence artificielle, conçu pour détecter et identifier des cibles en temps réel, même en présence de brouillage électronique, améliorant ainsi la précision et l'efficacité des opérations militaires.

[84] Le *Droid TW 12.7* est un complexe robotique terrestre de reconnaissance et de combat, développé par l'entreprise ukrainienne DevDroid. Monté sur une plateforme à chenilles, il est équipé d'une mitrailleuse Browning de calibre 12,7 mm et peut être télécommandé via une tablette

autonomes, requièrent toujours l'intervention humaine pour valider leurs actions. Le premier étant souvent affilié au réseau Delta[85] et nécessitant une puissance de calcul considérable, il est rapidement limité dans ses fonctionnalités de détection et de ciblage via des caméras optiques, voire thermiques. Cette dimension pose la question de la miniaturisation et l'intégration de ces options dans des drones légers ou compacts, avec une incidence sur leur autonomie énergétique, d'autant plus vulnérables s'ils doivent être alimentés par des systèmes plus lourds ou stationnaires[86]. Ainsi, loin de l'image d'une automatisation complète du champ de bataille, ces technologies viennent en soutien de la prise de décision humaine.

Si l'intelligence artificielle militaire peine encore à atteindre un niveau décisionnel avancé, elle joue en revanche un rôle de plus en plus déterminant dans l'optimisation des systèmes de commandement et de contrôle (C2). L'Ukraine, notamment, s'est distinguée par l'intégration de logiciels conçus pour améliorer la gestion de son artillerie et de ses drones. Le système de cartographie *Kropyva*, développé localement, est non seulement employable depuis de simples tablettes Android, mais il permet également de coordonner en temps réel les frappes d'obusiers et d'optimiser les trajectoires balistiques en fonction des conditions de terrain[87]. De son côté, la *plateforme Styx* offre un cadre algorithmique de gestion des essaims de drones permettant une meilleure synchronisation des actions offensives. Dans ce réseau coordonné, chaque drone est capable de planifier ses propres mouvements et d'anticiper les comportements des autres membres de l'essaim. Ce projet tout droit sorti de la *startup* ukrainienne Swarmer, a été soutenu à hauteur de 50 000 dollars par le cluster gouvernemental ukrainien BRAVE1[88], de technologies locales, mais aussi depuis septembre 2024, par la levée de fonds de la société américaine R-G.AI, aux côtés de plusieurs *venture capital*[89]. Ces développements illustrent l'une des principales contributions de l'intelligence artificielle militaire moderne : non pas remplacer l'homme dans la prise de décision, mais lui fournir des outils permettant d'accélérer et d'affiner ses choix tactiques.

3. Les passages à l'échelle de l'IA militaire : entre potentialités opérationnelles et réalités d'intégration contrariées

Si l'autonomie décisionnelle des systèmes d'armes reste encore entravée par d'importantes limites, l'intelligence artificielle s'est néanmoins imposée comme un levier d'optimisation au sein des forces armées. Son intégration progressive irrigue désormais l'ensemble du spectre opérationnel, de la planification des opérations jusqu'au soutien logistique, en passant par le renseignement et la gestion du feu. Cette montée en puissance traduit une mutation doctrinale où la machine assiste l'homme dans la prise de décision, sans pour autant s'y substituer. Il convient ainsi d'examiner les champs d'application actuels de l'intelligence artificielle militaire et les bénéfices opérationnels qu'elle génère.

ou une manette de jeu. Conçu pour effectuer des missions de reconnaissance et de combat en première ligne, il assure une précision de tir élevée même dans des conditions difficiles

[85] Le Réseau Delta est un système de gestion du champ de bataille développé par le Centre pour l'Innovation et le Développement des Technologies de Défense du ministère ukrainien de la Défense, en collaboration avec l'organisation *Aerorozvidka*. Les premiers tests ont eu lieu en 2017, et le système est devenu pleinement opérationnel en août 2022.

[86] « Ukrainian Forces Get an AI-Powered Saker Scout Drone, and Its Algorithms Can Solve an Important Problem », *Defense Express*, 4 septembre2023,https://en.defenceua.com/weapon_and_tech/ukrainian_forces_get_an_ai_powered_saker_scout_drone_and_its_algorithms_can_solve_an_important_problem-7842.html.

[87] Raido Saremat, "Punching above Your Weight with the Use of Modern Technology", *Vegvisir Blog*, 2024, https://www.vegvisir.ee/blog/punching-above-your-weight-with-the-use-of-modern-technology.

[88] BRAVE1 est une initiative ukrainienne lancée en 2023, réunissant des acteurs gouvernementaux, industriels et technologiques pour accélérer le développement et le financement de solutions de défense innovantes, notamment en matière de drones, d'intelligence artificielle et de guerre électronique.

[89] Le capital-risque (*venture capital*) est une forme de financement apportée par des investisseurs à des startups ou entreprises innovantes à fort potentiel de croissance, en échange d'une prise de participation au capital, avec un niveau de risque élevé mais des perspectives de rendements importants.

a) L'IA comme catalyseur d'efficacité opérationnelle : des champs d'application différenciés selon les besoins capacitaires et doctrinaux

Comme il a pu être souligné lors du passage en revue de l'état de l'art s'agissant des acteurs principaux de l'innovation en matière d'intelligence artificielle, plusieurs champs des opérations bénéficient aujourd'hui d'une assistance numérique et permettent d'anticiper les apports nécessaires au passage à l'action. L'optimisation des chaînes logistiques et du soutien permet ainsi de doter les armées de capacités nouvelles, réfléchies selon un ensemble cohérent allant des effectifs humains aux équipements, et suivant une doctrine d'emploi clairement délimitée. Le soutien vient notamment dans les bénéfices accordés aux personnels soignants dans leurs prises en charge des patients militaires, particulièrement l'identification et l'anticipation des facteurs de risques sur le terrain.

Ce champ, catégorisé dans l'acronyme DORESE (Doctrine, Organisation, RH, Equipements, Soutien, Entrainement), s'axe sur les capacités de simulations de l'intelligence artificielle, qu'il s'agisse de la formation et du recrutement à partir d'analyse et d'apprentissage automatique, ou de simulateurs réalistes d'entrainement pour mettre les soldats en condition (*wargame*, exercice terrain augmenté à des fins d'aguerrissement, comportements des ennemis et alliés enrichis des RETEX). Les robots logiciels et autres *chabots* optimisent et programment quant à eux les ressources consommables, les traitements de tâches ingrates et la maintenance prédictive sur les équipements et les infrastructures des soldats à l'image du *Système Rora*[90], présenté par l'AMIAD[91] au salon d'*Eurosatory 2024*. Venant en aide au personnel de la maintenance, ce système fonctionne hors connexion, ce qui est particulièrement efficace lorsque les forces sont projetées comme en opérations extérieures (OPEX). Il identifie la pluralité du matériel et la références des pièces à partir d'une mémoire d'images, remplaçant la chaine AIP (autonomie initiale de projection), pour gérer les stocks pré positionnés et le soutien immédiat en logistique. L'application est téléchargeable depuis un smartphone et transforme les photographies en vecteurs qui sont dès lors comparés dans la base de données d'identification. Egalement déployée dans l'US Air Force dès 2018 via la société C3IoT[92], les systèmes d'intelligence prédictive ont permis de réduire la maintenance curative des *F-16* et *AWACS E-3 Sentry* de 20 à 50 %, augmentant ainsi leur disponibilité de 40 %. Ces usages permettent donc de renforcer la résilience opérationnelle des forces armées.

La planification opérationnelle ainsi que l'analyse prédictive face à l'adversaire sont un autre échelon de cet apport des technologies de l'IA, notamment lorsqu'il s'agit de repérer les « conduites récurrentes », les fameuses « *patterns of life* »[93]. Les données croisées et rattachées à des cibles accumulent ainsi des signatures radars et électromagnétiques, de même qu'une reconnaissance imagée des comportements passés chez l'ennemi, afin d'anticiper une partie de ses actions futures. Ces échantillons numériques permettent d'augmenter significativement la boucle OODA (Observer, Orienter, Décider, Agir) par des capteurs directement liés aux officiers chargés d'opérer un choix dans la conduite des opérations. La mise en réseau s'établit donc par gradation entre les divers appareils et centres de commandement, le tout en traitant une quantité impressionnante de données en un temps record, sur plusieurs objectifs.

[90] Ministère des Armées, *TaiDX l'IA de défense*, YouTube, 17 juin 2024, extrait à 30 min, Bertrand Rondepierre : « Système Rora », https://www.youtube.com/watch?v=6IuGTTYeCS8.

[91] L'Agence ministérielle de l'intelligence artificielle de défense (AMIAD) est une entité française créée en mai 2024, sous l'égide du ministère des Armées, avec pour mission de développer et d'intégrer des solutions d'intelligence artificielle dans les programmes militaires, renforçant ainsi la souveraineté technologique de la France.

[92] C3 IoT était le nom utilisé par la société américaine C3.ai entre 2016 et 2019, reflétant son orientation vers l'Internet des objets (IoT). Fondée en 2009 par Thomas Siebel, l'entreprise s'est initialement concentrée sur la gestion des empreintes carbone des entreprises, avant de se spécialiser dans les solutions d'intelligence artificielle et d'IoT pour divers secteurs industriels. En 2019, elle a adopté le nom C3.ai pour mettre en avant son expertise en intelligence artificielle.

[93] Les "Patterns of Life" (PoL) ou « conduites récurrentes » désignent, dans le domaine des IA militaires, l'analyse et la modélisation des comportements habituels d'un individu, d'un groupe ou d'une entité (véhicule, unité militaire) sur une période donnée. L'IA exploite ces données pour détecter des anomalies, anticiper des actions ennemies ou automatiser le ciblage, notamment dans les missions de renseignement, surveillance et reconnaissance (ISR).

L'idée d'une « *Hyperwar* » telle que l'ont développé les auteurs John Allen et Amir Husain dans leur ouvrage éponyme de 2018[94], n'est donc pas si surprenante, bien qu'extrapolée à outrance. Renforçant l'agilité du système de commandement, qu'il s'agisse de la phase de planification ou de conduite, ce processus opère un décloisonnement, un filtrage et une mise en lumière des informations nécessaires, de sorte que le travail collaboratif s'en trouve fluidifié. Comme le souligne ainsi le Comité d'éthique de la défense dans son *Avis sur l'usage des technologies d'intelligence artificielle par les forces armées*, publiée le 14 janvier 2025 : en phase d'observation *« les systèmes traitant une importante quantité de données sur une durée longue »* vont permettre de *« dissiper d'autant le brouillard de la guerre (activité suspecte, présence d'éléments détectés, présence de civils) »* et de définir *« le point clé de la manœuvre à effectuer »*[95]. La phase d'orientation sera quant à elle largement décloisonnée par une grille d'analyse prenant en compte l'aspect évolutif du champ de bataille, d'après un historique opérationnel enrichi des expériences passées.

Enfin, l'un des jalons qui semble aujourd'hui le plus s'épanouir grâce aux apports de l'intelligence artificielle, reste la branche renseignement ISR (renseignement, surveillance, reconnaissance), dont les armées dépendent activement pour leurs compréhensions des intérêts adverses. Dans un paysage géopolitique caractérisé par une multitude d'informations souvent contradictoires, la capacité à trier, analyser et diffuser des données pertinentes est devenue primordiale. Grâce aux algorithmes sophistiqués, le cycle de renseignement, souvent réduit par la masse des données et le chaos ambiant, s'enrichit d'outils permettant de détecter des signaux faibles et d'anticiper les failles doctrinales adverses. Le gain de vélocité en amont des manœuvres, ainsi que l'intoxication des informations, permettent donc de tromper l'adversaire tout en se préservant, non seulement de la manipulation par les capteurs ennemis à l'aide de signaux mensongers, mais également dans le champ informationnel (*Infox, Deepfakes, PsyOps*[96]) et dans l'adaptation aux variables adverses (faiblesses ou failles doctrinales). La machine assiste ainsi la boucle ORED (Orientation, Recueil, Evaluation, Diffusion), explorant par du « *datamining* »[97] les métadonnées à traiter, en se calquant sur les plans prédéfinis et les besoins fondamentaux qui lui ont été fournis pour identifier les éventuels manques de connaissance.

L'apprentissage multi-agents par renforcement (Multi-Agent Reinforcement Learning - MARL) qui sied de plus en plus aux manœuvres ISR, combine ainsi le nombre de cibles, leur contrainte d'accès, ainsi que l'espace-temps des capteurs (drones ou autres). Un exemple parlant de système prédictif lancé dans le cadre des appels à projets d'intelligence artificielle par l'AID[98], est le *modèle AURORA*. Développé par Synapse Défense[99] et l'Institut de recherche technologique Saint Exupéry entre 2020 et 2021, il illustre parfaitement comment l'intelligence artificielle peut optimiser la collecte et l'analyse des données pour assister la prise de décision. Ce système ne se contente pas de fournir des résultats, il explicite également les raisonnements sous-jacents à chaque hypothèse, créant ainsi une synergie renforcée entre l'homme et la machine dans des solutions tactiques collaboratives.

---

[94] Dans son ouvrage *Hyperwar: Conflict and Competition in the AI Century*, le général John R. Allen introduit le concept de hyperwar, désignant une forme de conflit où l'intelligence artificielle et les systèmes autonomes accélèrent drastiquement le cycle décisionnel militaire, réduisant ou éliminant l'intervention humaine, ce qui modifie profondément la nature et la conduite des opérations militaires.

[95] Comité d'éthique de la défense, *Avis sur l'usage des technologies d'intelligence artificielle par les forces armées*, ministère des Armées, 14 janvier 2025, p. 13, section « L'aide à la décision, voire la décision pour la planification », https://www.defense.gouv.fr/sites/default/files/ministere-armees/20250114_np_comedef_avis-sur-l%27usage-des-technologies-d%27intelligence-artificielle-par-les-forces-armees.pdf.

[96] Psy Ops (Psychological Operations) désigne l'ensemble des opérations psychologiques menées par des acteurs militaires ou politiques pour influencer les perceptions, les émotions et les comportements d'un public ciblé. Utilisées en temps de guerre ou de crise, ces stratégies incluent la désinformation, la propagande, les campagnes de manipulation médiatique et l'usage des *deepfakes*, visant à affaiblir l'adversaire ou à mobiliser une population.

[97] Le *datamining* (ou exploration de données) est un processus d'analyse automatisée de grands volumes de données visant à identifier des modèles, tendances ou corrélations utiles, souvent utilisé en intelligence artificielle, en marketing et en renseignement.

[98] L'Agence de l'innovation de défense (AID) est une entité française créée le 1er septembre 2018, placée sous la responsabilité du Délégué général pour l'armement (DGA), ayant pour mission de coordonner et de piloter l'innovation et la recherche scientifique et technique au sein du ministère des Armées.

[99] Synapse Defense est une société par actions simplifiée (SAS) française, créée le 1er mars 2018. Elle se spécialise dans les prestations de services et de conseil liées aux opérations aériennes militaires, notamment le soutien à l'entraînement, l'évaluation de la performance et la création de contenus pédagogiques.

L'assistant virtuel multi-agents vient en aide au *Sensor Warden*, sorte de coordinateur complémentaire des capteurs hétérogènes de l'armée de l'Air, notamment dans les missions qui incluent du renseignement, de la surveillance, du ciblage et de la reconnaissance (ISTAR).[100] De même, le marché *TORNADE*, lancé en 2022 par la DGA en collaboration avec Preligens[101], a pour objectif d'équiper les forces armées d'outils capables de traiter de vastes masses de données issues de sources multiples. Ce système est une suite d'outils d'analyse du renseignement d'origine image visant à la surveillance de zones ou la réalisation de cartographie réactive, le tout à fins de renseignement et de préparation de missions. Mis en exploitation lors de l'exercice HEMEX ORION 2023[102], TORNADE a permis à la 11e Brigade parachutiste de bénéficier d'un soutien tactique renforcé, démontrant ainsi l'impact concret des technologies d'intelligence artificielle sur le terrain.

b) Le commandement et le contrôle de l'IA (C2IA) et l'autonomisation des chaines de commandement : entre résistances doctrinales et complexité d'intégration

Le domaine du renseignement multicouche, intégrant divers capteurs, profite pleinement des avancées de l'intelligence artificielle. À l'inverse, les systèmes de commandement et de contrôle (C2) accusent un retard malgré plusieurs tentatives d'innovation et les efforts de passage à l'échelle. Cette situation s'explique par un ensemble de freins qui ralentissent le processus décisionnel des officiers. D'une part, les doctrines d'emploi varient d'un pays à l'autre, et d'autre part, l'absence d'un cadre légal global et de juridiction officielle sur ces modèles de commandement rend leur mise en œuvre complexe. De plus, le manque de ressources adaptées pour appréhender la totalité du champ de bataille constitue un obstacle majeur. Dans le cadre de l'écosystème C2IA[103] développé par les armées françaises, les systèmes d'information opérationnels et de communication (SIOC) jouent un rôle central. Ces systèmes permettent la corrélation des données issues de diverses sources afin d'offrir une vision d'ensemble de la situation. Différentes couches de sécurité, identifiées sous l'appellation SSi, interviennent pour protéger les données sensibles. Elles détectent les anomalies et opèrent dans des environnements tactiques et stratégiques interalliés, notamment au sein de l'OTAN ou de l'Union européenne, limitant ainsi les risques de compromission lors d'éventuelles cyberattaques. Parallèlement, des sous-systèmes dits « hermétiques » sont conçus pour fonctionner de manière totalement isolée du reste du réseau, garantissant ainsi une continuité opérationnelle même en cas de déconnexion ou de compromission du système global.

Testé en 2020 par les FAG (Forces Armées en Guyane), le *Programme KEOS* s'inspire de ces modèles afin de faciliter les échanges d'informations à divers niveaux hiérarchiques (stratégique, opérationnel, tactique), et entre diverses forces armées allant du cadre interarmées au multinational. Prenant le revers du « *Machine Learning* », *KEOS* s'inspire des modèles logiques de l'intelligence artificielle symbolique pour soumettre des hypothèses purement transparentes à l'égard de son intermédiaire humain[104]. Cet outil combine donc des méthodes telles que le cumul d'analyse sémantique et de lecture d'image, de la compréhension GEOINT, de la simulation, ainsi qu'un module d'intelligence artificielle multi-agents. Censé atteindre une phase ultérieure au Centre de Planification et de Conduite des Opérations (CPCO) pour un agrandissement de la manœuvre, ce projet a toutefois été stoppé en raison de plusieurs écarts doctrinaux entre les divers partis, outre les importants coûts budgétaires. Les

[100]Agence de l'innovation de défense, *2 projets retenus dans le cadre de l'appel à projets d'Intelligence Artificielle 2020-2021*, Ministère des Armées,1er mars 2021, https://www.defense.gouv.fr/aid/actualites/2-projets-retenus-cadre-lappel-a-projets-dintelligence-artificielle-2020-2021.
[101] Preligens est une entreprise française fondée en 2016 par Arnaud Guérin et Renaud Allioux, spécialisée dans le développement de solutions d'intelligence artificielle pour l'analyse automatisée de données géo spatiales, notamment pour les secteurs de la défense et du renseignement.
[102] L'exercice HEMEX ORION 2023 était un entraînement militaire interarmées de grande envergure, organisé par la France entre février et mai 2023, visant à préparer les forces armées à des opérations de haute intensité. Il s'est déroulé en plusieurs phases, notamment dans le Sud de la France, avec des débarquements amphibies à Sète et des manœuvres terrestres jusqu'à Castres, ainsi que dans le Nord-Est, couvrant des zones comme la Marne, l'Aisne et les Ardennes (12 000 militaires et 14 pays réunis).
[103] Le Commandement et Contrôle des Opérations Interarmées (C2IA) est un concept visant à améliorer la prise de décision des forces armées françaises en automatisant les tâches répétitives et à faible valeur ajoutée, permettant ainsi aux commandements de se concentrer sur l'analyse et l'élaboration de solutions opérationnelles. L'IA y joue un rôle central depuis le consortium de 2019, composé de plusieurs entreprises ayant envisagé une solution destinée à l'assistance du CPOIA et du CPCO dans la prise de décision.
[104] Mars Attaque. « Innovation et défi du C2IA : Vers un commandement augmenté par l'intelligence artificielle. » *Mars Attaque*, 15 mars 2020. https://mars-attaque.blogspot.com/2020/03/innovation-defi-c2ia-commandement-cpoia-intelligence-artificielle.html.

armées procèdent à ce stade à une adoption prudente et progressive des capacités d'intelligence artificielle. Alors que l'innovation technologique de demain vise à atteindre une forme « d'intelligence augmentée », ce souhait repose avant tout sur une architecture complexe, inévitablement ambiguë, où la machine se met *in fine* pleinement au service de l'homme. Dans ce cadre, l'intelligence artificielle se charge du traitement des données brutes et de la gestion logistique, permettant aux décideurs et aux exécutants de se recentrer sur des problématiques plus profondes, libérant par suite la chaine OODA de son habituelle lenteur. En outre, cette vision prospective repose principalement sur une intégration multi-milieux multi-champs (M2MC) unifiée, combinant les domaines terrestre, maritime, aérien, spatial et cybernétique. Elle s'appuie donc sur une coordination en temps réel d'effecteurs autonomes, tels que des drones ou des robots terrestres.

Dans cette lignée, le *programme SCAF* (système de combat aérien du futur), développé respectivement par la France, l'Allemagne, l'Espagne, et plus récemment le partenaire Belge, vise à renforcer la coopération européenne en matière de défense ; il fait pourtant face à des défis structurels majeurs dans les divergences d'emplois. S'inscrivant dans une logique de combat collaboratif dans un environnement M2MC, il intègre justement des technologies d'intelligence artificielle avancées pour maximiser l'interconnexion et la prise de décision en temps réel sur les théâtres d'opération. Encore en phase de développement et prévu pour l'horizon 2040, ce « système des systèmes » doit comprendre des avions de chasses furtifs, des drones d'appui et d'accompagnement, ainsi qu'un *cloud* chargé de relier les vecteurs entre eux pour fournir de la donnée. Les dernières déclarations du sénat Français, qui fait ici montre de querelles d'intérêts entre les divers partis allant des problématiques d'exportation, de souveraineté mais aussi de mésententes sur le produit lui-même, tels que des détails ayant trait aux performances technologiques dans un milieu aérien hautement contesté, relèvent toutefois de l'incertitude quant au futur du projet[105].

Une telle orchestration fait encore défaut dans l'écosystème français, mais est déjà bien avancée outre-Atlantique. Aux États-Unis, diverses infrastructures ont été développées pour répondre aux besoins croissants d'une circulation augmentée de l'information, qu'il s'agisse des soldats déployés en première ligne ou des centres décisionnels opérant à l'arrière. Pour parvenir à cet objectif, il est essentiel de disposer d'une masse critique de capteurs interopérables malgré leur diversité en termes de nature et de mission. Ce concept aboutit à celui du *combat cloud*[106], où les plateformes militaires ne se limitent plus à leurs fonctions classiques d'effecteurs mais deviennent également des capteurs et relais C2. Ces plateformes interconnectées jouent un rôle multiple en tant que passerelles instantanées d'information. Cette mise en réseau optimise leur agilité collaborative, au détriment toutefois de leur efficacité individuelle lorsqu'elles opèrent de manière isolée. Ce modèle représente ainsi le sommet de l'optimisation des moyens et des champs d'application.

On en veut pour preuve, l'initiative *Project Convergence*, destinée à moderniser le commandement et le contrôle (C2) américain grâce à l'intelligence artificielle dans un cadre M2MC, qui a conduit au récent exercice *Capstone-4* (PC-C4) à Fort Irwin et Camp Pendleton. Lancé dès 2020 sous l'égide de l'Army Futures Command, ce projet a mobilisé près de 4 000 militaires interarmes issus non seulement des États-Unis, mais aussi de pays alliés tels que la France, le Royaume-Uni, le Canada, l'Australie et le Japon. Cet exercice ambitieux visait à mettre en œuvre une défense multiniveau au sein d'une coalition internationale. Plusieurs systèmes d'armes ont été projetés simultanément contre des cibles situées dans une zone défendue afin de maximiser les chances de destruction et d'exploiter pleinement l'efficacité des plateformes interconnectées. À titre d'exemple, un avion *F-35* de l'US Navy a été utilisé comme capteur pour détecter des cibles maritimes. Les informations recueillies ont ensuite été

[105] Laurent Lagneau, *Selon le Sénat, les divergences avec Berlin font douter de l'avenir du Système de combat aérien du futur*, Zone Militaire - Opex360, 1er décembre 2024, https://www.opex360.com/2024/12/01/selon-le-senat-les-divergences-avec-berlin-font-douter-de-lavenir-du-systeme-de-combat-aerien-du-futur/.

[106] Le *Combat Cloud*, conceptualisé par le Lt Gen David A. Deptula en 2016 dans un article du *Mitchell Institute for Aerospace Studies*, est un paradigme opérationnel interconnectant en temps réel les systèmes militaires via un réseau maillé. Il optimise le partage des données, la coordination interarmes et la prise de décision, renforçant ainsi l'efficacité des opérations multi domaines.

transmises à une unité de gestion de bataille de l'US Air Force avant d'être relayées vers un système de missiles de l'US Army pour engager la cible[107]. A cet égard, *les* systèmes *MIST (Multimodal Input Surveillance & Tracking)* et *JAWS (Joint All-Domain Warfighting Software),* utilisant des algorithmes d'apprentissage profond et des pipelines avancés de gestion des données[108], ont démontré leur capacité à assister efficacement les opérateurs humains dans la détection et la priorisation des cibles critiques[109].

c) Le mode dégradé

Si toutefois le développement de tels usages constitue un atout stratégique pour les armées, une zone d'ombre reste à combler, celle du mode dégradé qui s'accorde avec la complexité des milieux et de l'environnement qui englobent le combat, au-delà des aléas comportementaux de l'ennemi. La prédiction n'est pas une mince affaire, d'autant plus quand il s'agit d'un cadre militaire intégrant une coalition. Plusieurs problématiques se présentent alors, dont la nécessité de s'accorder clairement sur des normes d'emplois de l'intelligence artificielle, ce qui tend à être confus lorsque diverses écoles de pensées viennent se côtoyer en amont des démarches opératives : si on considère l'approche prudente de la France sur l'usage des IA militaires, comme mentionné dans la Loi de Programmation Militaire 2024-2030, celle-ci doit demeurer une *« IA de confiance »*[110]. De même le Rapport de la Task Force IA de septembre 2019, stipule bien que : *« la France n'envisage pas de développer des systèmes pleinement autonomes, échappant totalement au contrôle humain dans la définition et l'exécution de sa mission »*[111]. Par continuité elle appuie récemment sur le principe des systèmes d'armes létaux avec intervention humaine appropriée (SALIA) ; avec plus de liberté, les Etats-Unis considèrent pour leur part, que le développement des systèmes d'armes létaux autonomes (SALA) doit être, certes encadré dans le respect du droit de la guerre et des normes en vigueur, mais toutefois pleinement exploité s'il rend la frappe plus chirurgicale. La Directive 3000.09 du DoD[112] insiste ainsi sur le fait d'exploiter pleinement et à bon escient, toutes formes d'armes autonomes, tant qu'un opérateur reste en capacité de désactiver la frappe, en accord avec son jugement.

Les nuances, aussi frêles soient elles, participent ainsi aux désaccords, même interalliés, dans les conceptions de ce qui compose une limite ou une ligne rouge à ne pas dépasser. Ces divergences nourrissent des barrières évidentes aux bon fonctionnement et à la pleine intégration des capacités de l'intelligence artificielle au cœur des opérations. De même, « l'effet falaise », qui désigne un risque critique de recours excessif du commandement aux prédictions artificielles et aux systèmes d'armes autonomes qui en dépendent, laisse entrevoir d'inquiétantes failles pour les soldats, si les systèmes se mettaient à dysfonctionner. Dès lors, la planification des opérations doit pouvoir être envisagée en dehors du cadre purement technologique, s'appuyant à nouveau sur les usages et les pratiques classiques de la guerre au-delà de l'ultra connectivité. S'il advenait qu'un blocage se déclare sur les infrastructures militaires, la formation initiale du soldat devrait pouvoir suffire à la reprise du cours normal des opérations, empêchant ainsi d'aboutir à un cloisonnement handicapant et dangereux pour la poursuite des objectifs.

---

[107] Spc. Jackson Gray, *Project Convergence Capstone 4 works to integrate joint, multinational defense systems*, U.S. Army, 27 février 2024, https://www.army.mil/article/274045/project_convergence_capstone_4_works_to_integrate_joint_multinational_defense_systems.

[108] Chaînes de traitement automatisées permettant de collecter, analyser et transmettre des informations en temps réel.

[109] Gouvernement du Canada, *RDDC participe à l'expérience multinationale Projet Convergence Capstone 4*, 15 novembre 2024, https://science.gc.ca/site/science/fr/blogues/science-pour-defense-securite/rddc-participe-lexperience-multinationale-projet-convergence-capstone-4.

[110] Une « IA de confiance », selon les critères français, repose sur trois principes fondamentaux : explicabilité (transparence des décisions prises par l'algorithme), robustesse (fiabilité et résistance aux erreurs ou attaques), et éthique (respect des valeurs humaines et des cadres juridiques, notamment en matière de biais et de protection des données).

[111] Ministère des Armées, *Rapport de la Task Force IA*, septembre 2019, section « 2.1 Un cadre éthique et juridique robuste pour le ministère des Armées », p. 9, https://www.defense.gouv.fr/sites/default/files/aid/20200108-NP-Rapport%20de%20la%20Task%20Force%20IA%20Septembre.pdf.

[112] U.S. Department of Defense, *DoD Directive 3000.09: Autonomy in Weapon Systems*, 25 janvier 2023, https://www.esd.whs.mil/portals/54/documents/dd/issuances/dodd/300009p.pdf.

Titre III : Menaces et fragilités : les véritables défis dans la maitrise des technologies de l'intelligence artificielle

L'ascension rapide de l'intelligence artificielle dans les architectures de défense et les mécanismes d'influence fait naître une double illusion : celle d'un outil maîtrisé et celle d'une puissance affranchie des failles humaines. Pourtant, ces technologies demeurent intimement liées à leurs fragilités structurelles : ruptures informationnelles, dépendance aux infrastructures critiques, vulnérabilités cyber, mais aussi asymétries éthiques où l'intelligence artificielle devient parfois instrument d'oppression ou vecteur d'ingénierie sociale. Dans l'ombre des algorithmes se jouent aussi des luttes d'accès aux ressources matérielles et énergétiques, révélant une nouvelle cartographie du pouvoir, où celui qui contrôle le silicium et les données impose sa cadence au monde. Maîtriser l'intelligence artificielle, c'est d'abord composer avec ses points de rupture, techniques, humains, écologiques qui, loin d'être résiduels, définissent ses limites opérationnelles et stratégiques.

1. Données, systèmes et réseaux : l'IA face à sa propre vulnérabilité

Ainsi, tandis que l'intégration progressive de l'intelligence artificielle dans les systèmes militaires et décisionnels semble esquisser les contours d'une puissance accrue, cette illusion d'autonomie technique masque des fragilités systémiques profondes. Derrière l'apparente rationalité algorithmique, l'intelligence artificielle repose sur un triptyque vulnérable : données incertaines, réseaux exposés, infrastructures centralisées. Autant d'éléments dont l'altération peut renverser la machine, faisant vaciller l'édifice sur lequel repose cette nouvelle architecture du pouvoir.

a) La dépendance aux données comme faiblesse

Il est souvent dit que l'intelligence artificielle agit comme un accélérateur, un puissant outil de tri qui simplifie et fluidifie le traitement des tâches subalternes. Cette tentation d'automatisation s'impose d'autant plus dans des environnements exigeants comme les administrations publiques ou les armées, où l'empilement des procédures alourdit chaque opération. Pourtant, cette dynamique vertueuse ne repose que sur une condition essentielle : l'accès aux données, à la fois en abondance et en qualité. Car c'est bien dans cette matière brute que l'intelligence artificielle puise sa vitalité, se nourrissant de volumes massifs d'informations pour perfectionner ses processus et affiner ses réponses. Derrière cette mécanique d'apprentissage, un parcours rigoureux se déploie : collecte, filtrage, nettoyage, puis annotation des données, autant d'étapes qui garantissent la fiabilité et la diversité des ensembles exploités. C'est ce cheminement qui façonne la transition d'un simple modèle algorithmique vers un véritable agent opérationnel. Dans le domaine des systèmes d'armes, cet accès à la donnée se heurte cependant à une réalité contraignante : la domination des formats propriétaires[113], verrouillés par les industriels de la défense et les fabricants de matériels. Ces écosystèmes cloisonnés, parfois structurés en silos ou réservés à un usage exclusif, offrent certes l'avantage d'un contrôle rigoureux et d'une protection juridique par brevet, mais ils imposent, en contrepartie, une dépendance technologique coûteuse. Changer de solution ou migrer vers un autre fournisseur se révèle souvent ruineux, freinant la concurrence et restreignant la flexibilité opérationnelle des forces.

Face à ces blocages, les acteurs de la défense et de la sécurité cherchent à dessiner une nouvelle architecture de partage informationnel. L'enjeu est double : préserver la souveraineté des données stratégiques tout en fluidifiant leur circulation vers les industriels, les PME innovantes et les *startups,* dont l'agilité constitue un levier d'innovation indispensable. C'est sur cet équilibre délicat entre sécurité et ouverture que repose aujourd'hui la modernisation des outils numériques de défense. Dans cette optique a été lancé en 2022, le *projet ARTEMIS.IA (Architecture de Traitement et d'Exploitation Massive de l'Information*

[113] Les formats propriétaires désignent des formats de fichiers ou de données dont les spécifications techniques sont contrôlées par une entreprise ou une organisation, limitant leur compatibilité avec d'autres systèmes et nécessitant souvent des logiciels spécifiques pour leur utilisation.

Multi-Sources et d'Intelligence Artificielle), piloté par la société ATHEA, fruit d'une alliance entre Thales et Atos. Regroupant près d'une centaine de partenaires, ce programme vise à structurer un écosystème industriel robuste et souverain. Un kit de développement clé en main est ainsi mis à disposition des acteurs de l'industrie et de la recherche, leur offrant la possibilité de concevoir des applications conformes aux exigences du ministère des Armées (MINARM), tout en assurant la sécurité et la maîtrise des flux de données opérationnelles[114]. Après une phase de finalisation du projet en juin 2022, la plateforme, déployée à partir de 2023, s'est chargée de soutenir la fonction interarmées du renseignement. Ainsi, au cœur de ces efforts technologiques et industriels se dessine une ambition : dépasser l'enfermement dans les formats propriétaires pour bâtir une autonomie stratégique au service d'une efficacité opérationnelle renforcée.

L'optimisation, la conception, l'entrainement, la validation et l'amélioration continue des systèmes d'intelligence artificielle reposent avant tout sur la disponibilité de vastes ensembles de données d'entraînement, à la fois diversifiés et d'une qualité suffisante. Les algorithmes d'apprentissage et les fonctions de montée en puissance ne sont pertinents que lorsque les jeux de données qui les nourrissent reflètent un éventail représentatif de sources couvrant l'intégralité du spectre opérationnel et des scénarios plausibles. À défaut de cette masse critique d'informations variées, le champ d'analyse se rétrécit, bridant les capacités d'adaptation et de prédiction des intelligences artificielles, les empêchant d'exprimer leur plein potentiel. Le domaine des intelligences artificielles militaires n'échappe pas à ces contraintes, bien au contraire. Il en pâtit d'autant plus que la sécurité entourant leurs plateformes freine l'acquisition de données en comparaison de leurs équivalents civils, pour lesquels l'accès à des bases ouvertes est quasi illimité. Face à cette difficulté, le concept d'intelligences artificielles « frugales »[115], capables d'apprendre à partir d'un volume restreint de données, s'impose progressivement dans les milieux de la défense. Ces systèmes tirent davantage parti des retours d'expérience du terrain et des enseignements issus des exercices militaires, que des immenses bases de données habituelles.

À titre d'illustration, l'Armée de l'Air et de l'Espace française, grâce à ses drones *MQ-9 Reaper* déployés au Sahel, avait accumulé en mars 2021 plus de 40 000 heures de vidéos d'observation depuis 2014[116]. Une telle réserve de données constitue une ressource inestimable pour le développement d'outils intelligents. À l'inverse, d'autres puissances souffrent encore d'une carence criante en matière d'observations issues du terrain. La Chine, en particulier, n'a pas été engagée dans un conflit majeur depuis la guerre sino-vietnamienne de 1979. Cette absence d'expérience opérationnelle grève lourdement sa capacité à éprouver ses systèmes d'aide à la décision, qui demeurent balbutiants. Ces derniers se limitent encore largement à l'exécution de directives humaines, loin d'une réelle autonomie cognitive. Privée de données issues des conflits modernes et manquant de modèles de grande échelle pour le *machine learning*, l'APL voit ses simulations peiner à refléter le réalisme et la complexité du combat contemporain. Pour contourner cette faiblesse, les autorités chinoises ont cherché à compenser par la génération de données artificielles, issues de *wargames* informatisés et d'exercices simulés. Des systèmes comme *War Skull*[117] ou *Prophet* en sont les

[114] Benoit, Marie-Claude. « La Direction générale de l'armement attribue la réalisation de la plateforme ARTEMIS.IA à ATHEA. » *Actuia*, 19 juillet 2022. https://www.actuia.com/actualite/la-direction-generale-de-larmement-attribue-la-realisation-de-la-plateforme-artemis-ia-a-athea/#artemisia.

[115] La France a encadré l'IA frugale à travers le Référentiel général pour l'IA frugale, publié en juin 2024 par le ministère de la Transition écologique. Il définit une méthodologie pour mesurer et réduire l'impact environnemental des systèmes d'IA, s'inscrivant dans la Stratégie nationale pour l'intelligence artificielle (SNIA) et le plan France 2030.

[116] Arnaud. « Les drones MQ-9 Reaper atteignent 40 000 heures de vol au Sahel. » *Avions Légendaires*, 6 avril 2021. https://www.avionslegendaires.net/2021/04/actu/les-drones-mq-9-reaper-atteignent-40000-heures-de-vol-au-sahel/.

[117] *War Skull* est un agent intelligent de prise de décision en combat, développé par l'Université nationale de technologie de la défense (NUDT) en Chine, sous la direction de Feng Yanghe. Créé pour optimiser la planification militaire dans des environnements complexes, il combine raisonnement cognitif, apprentissage supervisé, apprentissage d'ensemble et apprentissage par renforcement. Testé sur une plateforme de simulation de jeux de guerre, il a été entraîné pendant 136 jours, jouant plus de 160 parties par jour pour affiner ses stratégies. Lors du 3e Concours national de jeux de guerre, *War Skull* a remporté 22 victoires sur 22 face à des stratèges humains.

produits les plus emblématiques[118]. Cependant, cette approche n'est pas sans risques : l'accès parcellaire aux données réelles conduit à nourrir les intelligences artificielles d'informations biaisées, enfermées dans les limites des scénarios théoriques. En l'absence d'une confrontation à la brutalité et à l'imprévu du terrain, ces systèmes risquent de reproduire et d'amplifier des comportements déconnectés des réalités de la guerre moderne.

b) Brouillage et intoxication des données sur les capteurs

Si l'accès à une donnée abondante, fiable et maîtrisée conditionne l'efficacité des architectures d'intelligence artificielle, cette dépendance devient une faiblesse critique dès lors que l'ennemi en perçoit l'enjeu et s'efforce de la priver ou de la corrompre. Ce n'est plus seulement la rareté ou la clôture des écosystèmes propriétaires qui fragilise les systèmes, mais bien leur vulnérabilité face à une guerre cognitive et électronique où la donnée elle-même devient un champ de bataille. Sur le terrain, cette réalité s'impose avec une brutalité croissante. L'intoxication des capteurs, le brouillage des systèmes de navigation satellitaire (GNSS) ou la falsification des positions GPS ne relèvent plus de cas isolés : ils constituent désormais des armes tactiques à part entière, capables de paralyser des chaînes de décision intégrant l'intelligence artificielle. Le conflit ukrainien offre l'exemple le plus frappant de cette nouvelle donne. Dès les premières semaines de l'invasion russe, les forces de Moscou ont fait de l'aveuglement technologique de leurs adversaires une priorité. Drones désorientés par des signaux de localisation manipulés, liaisons satellitaires interrompues, systèmes de reconnaissance nourris d'informations erronées : sur l'ensemble du front, les Ukrainiens ont dû composer avec une guerre électronique d'une ampleur inédite.

Si le brouilleur *Krasukha-4*[119], déployé pour neutraliser les radars aéroportés et perturber les capteurs des drones occidentaux incarne cette stratégie sur le front Est, une autre technologie russe a récemment illustré la dangerosité de cette guerre invisible bien au-delà des champs de bataille : au tournant 2024, le système *Tobol* de brouillage satellite a été suspecté d'être à l'origine d'importantes perturbations GPS ayant frappé l'espace aérien dans diverses zones d'Europe. Pendant plusieurs jours, pilotes de ligne et unités de l'OTAN ont signalé des pertes de signaux et des dérives inexpliquées sur leurs outils de navigation. D'abord perçu comme un incident technique, l'événement s'est révélé être une manœuvre d'ingérence électronique. Officiellement conçu pour protéger les satellites russes des attaques cybernétiques, *Tobol* se révèle aussi capable de brouiller activement les signaux de navigation occidentaux, injectant une incertitude critique dans les opérations aériennes et terrestres. Le corridor de Suwałki ainsi qu'une partie des Pays Baltes et de la Pologne ont subi ces attaques, l'origine des signaux étant retracée comme émanant de la ville de Kaliningrad entre le 10 et le 16 janvier[120]. Ce brouillage, survenant à la frontière orientale de l'Europe rappelle que la guerre des données ne connaît plus de limites géographiques. L'Ukraine tente toutefois de riposter avec des contre-mesures adaptatives et des systèmes portatifs comme *Bukovel-AD* et *Kvertus*[121], bien que ces évènements de *jamming* aient déjà connus des précédents, en 2022 et en 2023, dans des zones d'intérêts stratégiques pour la Russie (Mer Noire, Mer Méditerranée, territoire Syrien).

Ces atteintes ne sont pas sans conséquences pour l'intelligence artificielle militaire, tributaire d'une géolocalisation et d'un flux constant de données exactes pour optimiser ses algorithmes. Privée de cette précision, ou pire, alimentée par des informations

[118] Fan, Ning, Zhu Mengying and Zhang Qiang. 2021. "远超阿尔法狗？'战远'成战远远助决策 '最强大远'" [Far more than Alpha Dog? "War Skull" becomes the "strongest brain" to assist decision-making on the battlefield]. 科技日报 [Science and Technology Daily], April 19. http://digitalpaper.stdaily.com/http_www.kjrb.com/kjrb/html/2021-04/19/content_466128.htm?div=-1.

[119] Le Krasukha-4 est un système de guerre électronique développé par la société russe KRET (Concern Radio-Electronic Technologies), une filiale de Rostec. Mis en service dans les années 2010, il est conçu pour brouiller les radars aéroportés, les satellites espions et les communications des drones, jouant un rôle clé dans la protection des infrastructures militaires russes contre les frappes de précision et la surveillance ennemie.

[120] Julien Lausson, « La Russie est suspectée d'avoir largement brouillé les GPS en Pologne, » *Numerama*, 18 janvier 2024, https://www.numerama.com/cyberguerre/1612064-la-russie-est-suspectee-davoir-largement-brouille-les-gps-en-pologne.html.

[121] *Bukovel-AD* et *Kvertus* sont des systèmes ukrainiens de guerre électronique utilisés pour neutraliser les drones ennemis. *Bukovel-AD* brouille les signaux de navigation et de communication des drones, tandis que *Kvertus* propose des brouilleurs portables interférant avec les transmissions radio et GPS, renforçant ainsi la défense aérienne ukrainienne.

corrompues, elle se retrouve non seulement inefficace, mais potentiellement dangereuse. Des frappes mal ajustées aux trajectoires de drones devenues erratiques, les décisions humaines, pilotées en partie par des traitements automatisés, se trouvent faussées à la source. L'opérateur n'est plus simplement confronté à une panne, mais à une incertitude constante : chaque donnée reçue est-elle encore le reflet du réel ou l'arme d'une désinformation savamment orchestrée ? Face à cette menace, les armées occidentales et notamment françaises, renforcent leurs capacités de résilience et d'authentification des flux. Le *programme SYMETRIE (Synchronisation des Moyens et des Effets dans la Tridimensionnalité)* vise précisément à doter les forces d'outils de renseignement électromagnétique (ROEM) capables de détecter, intercepter, localiser et neutraliser les signaux adverses (communications, radars) en synchronisant capteurs (drones, guerre électronique) et effecteurs (artillerie, hélicoptères) dans la profondeur (50-500 km) grâce à des technologies avancées de Thales et Airbus, renforçant la supériorité informationnelle dans les conflits de haute intensité. Il fonctionne en exploitant l'intelligence artificielle pour analyser rapidement les données multi capteurs, contrer le brouillage ennemi, et valider les observations via des dispositifs de « *cross-checking* » (capteurs optiques, radars, centrales inertielles), assurant des frappes précises et rapides. Lors de l'exercice Grand-Duc 2024, qui s'est déroulé du 15 au 29 mars sous l'égide du Commandement des Actions dans la Profondeur et du Renseignement (CAPR), le programme a été testé dans un scénario fictif de conflit symétrique, démontrant sa capacité à accélérer la boucle renseignement-feux, à neutraliser les tentatives d'aveuglement ennemies et à coordonner une coalition interarmées face à des défis réalistes comme le harcèlement ou les franchissements complexes[122]. Cette logique irrigue également les communications : le *Modem 21*[123], développé pour sécuriser les échanges satellitaires, n'assure pas seulement la continuité des flux, il garantit leur intégrité, empêchant ainsi l'infiltration de leurres dans les chaînes de décision.

c) La problématique de l'asymétrie : le cas de la dualité

Dans un tel contexte, la dépendance aux données ne se limite pas à un enjeu de protection contre le brouillage ou l'intoxication ; elle crée également un déséquilibre stratégique exploitable par des adversaires asymétriques ou étatiques. Alors que les armées occidentales investissent massivement dans l'intelligence artificielle pour optimiser la prise de décision et automatiser certaines capacités de combat, cette dynamique permet à des acteurs aux moyens plus limités de détourner à leur profit des technologies duales. La militarisation de systèmes initialement civils, tels que les drones de loisir ou les plateformes *open-source*, offre une alternative redoutable aux solutions sophistiquées des grandes puissances. Un exemple concret de cette adaptation est l'apparition, début septembre 2024, du *Dragon Drone* au sein des forces ukrainiennes. Ce drone, dérivé de modèles civils de loisir, a été modifié pour larguer des charges incendiaires de thermite sur des positions russes, notamment dans la région de Zaporijia ; la thermite, un mélange d'oxyde de fer et de poudre d'aluminium, brûle à des températures atteignant 2 500 degrés Celsius, capable de détruire équipements et fortifications ennemis[124]. Cette innovation, documentée par des vidéos diffusées sur des canaux officiels ukrainiens, illustre comment des technologies civiles peuvent être transformées en armes redoutables sur le champ de bataille.

L'intégration de l'intelligence artificielle dans ces plateformes confère un avantage supplémentaire aux belligérants. Des drones semi-autonomes, capables de recalculer leur trajectoire par analyse d'images plutôt que par navigation satellitaire, deviennent insensibles aux brouillages GNSS (Géolocalisation et Navigation par un Système de Satellites). De même, l'emploi de vols en essaim, synchronisant plusieurs unités pour saturer les défenses adverses, complique la lecture stratégique et l'anticipation des manœuvres ennemies. Dans un conflit de haute intensité, ces capacités pourraient neutraliser localement la supériorité

[122] Nathan Gain. « Un commandement, quatre missions et un premier cap pour les acteurs de la profondeur. » *Forces Operations Blog*, 17 octobre 2024. https://www.forcesoperations.com/un-commandement-quatre-missions-et-un-premier-cap-pour-les-acteurs-de-la-profondeur/.
[123] Thales. « Modem 21 et sécurisation des communications militaires par satellites : une innovation majeure. » *Thales*, 13 septembre 2023. https://www.thalesgroup.com/fr/monde/defense/news/modem-21-et-securisation-des-communications-militaires-satellites-une-innovation.
[124] Georges Lagueyrie. « Les 'Dragon Drones', ces nouveaux engins volants lance-flammes que les Ukrainiens utilisent face aux Russes. » *Le Figaro*, 11 septembre 2024. https://www.lefigaro.fr/international/les-dragon-drones-ces-nouveaux-engins-volants-lance-flammes-que-les-ukrainiens-utilisent-face-aux-russes-20240911.

conventionnelle, abaissant le seuil du recours à la force. L'usage massif de systèmes autonomes pourrait alors encourager une escalade dans l'emploi des frappes, certains acteurs se libérant des contraintes éthiques et juridiques pour engager des plateformes létales sans supervision humaine. Cette évolution impose une adaptation doctrinale et technologique rapide aux armées occidentales. La protection des données ne peut plus être pensée uniquement en termes de cyber sécurité ou de résilience électromagnétique ; elle doit aussi intégrer une dimension offensive, capable de perturber les réseaux adverses et de limiter leur accès à l'intelligence artificielle. Face à un adversaire qui exploite les failles de cette dépendance aux données, l'enjeu n'est plus seulement d'utiliser l'intelligence artificielle pour dominer le champ de bataille, mais d'empêcher que cette domination ne se retourne contre ceux qui la revendiquent.

2. L'envers du décor : les réalités écologiques et humaines de l'IA

Le 21 mars 2024 a marqué un tournant avec l'adoption par l'ONU d'une résolution pour des systèmes d'intelligence artificielle sûrs, sécurisés et dignes de confiance. Dans son allocution, Mme Thomas-Greenfield, ambassadrice des Etats-Unis auprès des Nations Unies, a déclaré : *« Réaffirmons donc que l'IA sera créée et déployée dans l'optique de l'humanité et de la dignité, de la sûreté et de la sécurité, des droits de l'homme et des libertés fondamentales »*[125]. Cette affirmation souligne l'impératif de gouverner ces technologies pour qu'elles ne compromettent ni l'environnement ni les valeurs humaines. Elle met en exergue les enjeux liés à la forte consommation énergétique et à l'extraction intensive des ressources, des préoccupations écologiques majeures. Simultanément, les dérives potentielles sur le plan social, telles que l'aggravation des inégalités et l'évolution des conditions de travail, sont au cœur des débats. Ainsi, cette déclaration sert de point de départ pour une réflexion approfondie sur l'envers du décor des intelligences artificielles. Elle invite l'observateur à interroger les impacts réels de ces technologies sur la planète et sur le tissu social. Ce tournant éthique appelle à une régulation stricte, garantissant que l'innovation ne se fasse pas au détriment de la durabilité.

a) L'empreinte environnementale : une IA énergivore

Si l'intelligence artificielle dépend des données dont elle se nourrit, elle est nécessairement soumise aux infrastructures qui lui offrent ce stockage en quantité. La gestion des masses dans le cadre des applications génératives employant le *Deep Learning* se comptent en centaines de gigabits[126], nécessitant l'accès à deux formats de management : les infrastructures de *Cloud* et d'*Edge Computing*. Ces deux formats présentent des avantages certains, le premier reposant sur le calcul et le stockage partagé des ressources accessibles via Internet, tandis que le second s'applique à la périphérie du réseau pour se rapprocher au plus près de la source des données. Bien que complémentaires, leurs aptitudes présentent des différences majeures s'agissant de l'optimisation des ressources et de la consommation énergétique. Alors que l'*Edge computing* réduit considérablement le traitement de données localement, le *cloud* garde un historique de stockage sur le long terme, ce qui accentue de toute évidence ses dépenses. Une solution émergente se dessine, celle des *cloud* hybrides dispersés, une approche qui combine les atouts du *cloud* public et privé, tout en répartissant les ressources géographiquement afin d'offrir un réponse plus flexible aux défis environnementaux. En distribuant les données de traitements, la distance entre les centres de données et les utilisateurs s'en voit diminuée, ce qui réduit aussi la latence et les énergies consommées pour leur transport. Parallèlement, les ordinateurs quantiques, et leurs capacités de calculs, deviennent les socles clés de la gestion des flux massifs indispensables aux intelligences artificielles, faisant de la synergie entre *cloud* hybrides dispersés et ordinateurs quantiques, un multiplicateur d'efficacité. Passant par la réduction du temps de calcul pour la résolution de problème, notamment via des super-ordinateurs, tout comme

[125] Nations Unies. « L'ONU adopte une résolution historique pour réglementer l'intelligence artificielle. » *Nouvelles ONU*, 21 mars 2024. https://news.un.org/fr/story/2024/03/1144211.

[126] Gigabit (Gb) est une unité de mesure de la vitesse de transfert de données équivalente à 1 milliard de bits. Utilisée principalement pour quantifier les débits des réseaux informatiques et des connexions Internet, elle se distingue du gigaoctet (Go), qui mesure la capacité de stockage. Par exemple, une connexion de 1 Gbps (gigabit par seconde) peut transmettre jusqu'à 125 mégaoctets de données par seconde.

l'optimisation des ressources allouées aux diverses tâches, ces outils vont permettre de mieux répartir des rôles. Il est encore trop tôt pour imaginer une telle puissance, et ces infrastructures sont encore au stade précoce de leur développement, toutefois ces solutions restent une piste plausible pour s'émanciper des tendances à la surconsommation. Les acteurs français détiennent à ce titre, près de 28% des parts de marché des infrastructures quantiques mondiales, principalement dans les processeurs[127]. Le projet *Proqcima* lancé début 2024 par l'Agence du numérique de défense (AND), développe ainsi deux prototypes d'ordinateurs quantiques universels à l'horizon 2032[128].

Ainsi, la question du stockage s'impose à présent comme un enjeu central des problématiques contemporaines, plaçant les États innovateurs et exploitants, au premier rang du changement. Cette responsabilité croissante a été réaffirmée lors du Sommet mondial sur l'intelligence artificielle, qui s'est tenu à Paris les 10 et 11 février, où a été officialisée une Coalition pour une intelligence artificielle écologiquement durable. Portée par la France, en collaboration avec le Programme des Nations Unies pour l'Environnement (PNUE) et l'Union Internationale des Télécommunications (UIT), cette initiative vise à inscrire l'intelligence artificielle dans une dynamique plus respectueuse des impératifs environnementaux. Comme l'a souligné Thomas Cottinet, directeur de l'Ecolab[129], *« le développement d'une IA durable et compatible avec nos objectifs environnementaux est possible, mais il impose de repenser nos usages et de privilégier des systèmes plus sobres »*[130]. Cette nécessité se justifie par l'impact considérable de l'intelligence artificielle générative sur les ressources naturelles : à chaque utilisation d'un prompt[131], près d'un demi-litre d'eau est consommé, tandis que l'Agence Internationale de l'Énergie (AIE) prévoit une multiplication par cinq de la consommation énergétique liée à l'intelligence artificielle dans les deux prochaines années. Par ailleurs, l'essor exponentiel de ces technologies engendre une production accrue de déchets électroniques, illustrant les effets délétères de l'intelligence artificielle sur les écosystèmes.

Consciente de ces défis, la France a été la première, à l'été 2024, à proposer un référentiel général de « l'IA frugale », recensant les bonnes pratiques visant à limiter son empreinte environnementale, notamment en matière de consommation d'eau, d'électricité et d'utilisation des matières premières. L'Europe, elle aussi, s'inscrit dans cette dynamique en ayant organisé, dès le 20 septembre 2024, un atelier d'experts consacré à la sobriété énergétique des outils d'intelligence artificielle en réseau[132]. Dans cette même perspective, l'Agence Internationale de l'Énergie a récemment exprimé son ambition de créer un observatoire dédié à l'analyse de l'impact de l'intelligence artificielle dans les facteurs de surconsommation, soulignant notamment l'augmentation attendue de plus de 75 % des besoins en électricité des *data centers* d'ici 2026, sous l'effet conjugué de l'essor des intelligences artificielles et des crypto monnaies[133].Face à l'essor fulgurant des technologies numériques et des besoins croissants en puissance de calcul, les géants du secteur se voient contraints d'adopter des solutions radicales pour répondre à cette demande exponentielle. Ainsi, en septembre 2024, Microsoft a annoncé la réactivation de l'unité numéro une de la centrale nucléaire de

[127] Institut Montaigne. « *Quantique : vers une logique de marché* » – *Résumé*. *Institut Montaigne*, Octobre 2024. https://www.institutmontaigne.org/ressources/pdfs/publications/resume-quantique-vers-une-logique-de-marche.pdf.

[128] Ministère des Armées. « Lancement du programme Proqcima et notification d'accords-cadres pour le développement d'ordinateurs quantiques universels. » *Ministère des Armées*, 6 mars 2024. https://www.defense.gouv.fr/sites/default/files/ministerearmees/06.03.2024%20Lancement%20du%20programme%20Proqcima%20et%20notification%20d%E2%80%99accordscadres%20pour%20le%20d%C3%A9veloppement%20d%E2%80%99ordinateurs%20quantiques%20universels.pdf.

[129] L'Ecolab, laboratoire d'innovation au service de la transition écologique, est une entité du Commissariat Général au Développement Durable (CGDD) du Ministère de la Transition écologique. Il a été officiellement créé en septembre 2021.

[130] Ministère de la Transition écologique. « Intelligence artificielle durable. » *Ministère de la Transition écologique*, 10 février 2025. https://www.ecologie.gouv.fr/actualites/intelligence-artificielle-durable.

[131]Instruction ou texte saisi par un utilisateur pour guider une intelligence artificielle dans la génération de réponses, d'images ou d'autres contenus. Il sert de point de départ pour orienter le modèle dans sa tâche.

[132] Commission européenne. "AI and Generative AI: Transforming Europe's Electricity Grid for a Sustainable Future." *Digital Strategy*, 22 février 2025. https://digital-strategy.ec.europa.eu/fr/library/ai-and-generative-ai-transforming-europes-electricity-grid-sustainable-future.

[133]Agence France-Presse. « L'AIE va lancer un observatoire sur l'impact de l'IA sur la consommation d'énergie. » *Connaissance des Énergies*, 11 février 2025. https://www.connaissancedesenergies.org/afp/laie-va-lancer-un-observatoire-sur-limpact-de-lia-sur-la-consommation-denergie-250211.

Three Mile Island, en Pennsylvanie, mise à l'arrêt depuis 2019[134]. Cette décision illustre l'urgence à laquelle sont confrontées ces entreprises, cherchant à garantir un approvisionnement énergétique suffisant pour alimenter des centres de données toujours plus énergivores.

Cependant, l'empreinte écologique des technologies de l'intelligence artificielle ne se limite pas à leur consommation électrique ou à l'énorme quantité d'eau nécessaire au refroidissement des centres de données. En amont de cette chaîne industrielle, l'extraction des ressources essentielles à la fabrication des semi-conducteurs et des puces électroniques constitue un véritable désastre environnemental. Parmi les sites les plus emblématiques de cette catastrophe figure Bayan Obo, en Mongolie-Intérieure. Ce gisement, appartenant à la Chine, est l'un des plus vastes au monde et représentait, en 2019, près de 45 %[135] de la production mondiale de terres rares[136]. Son exploitation entraîne une pollution massive des sols et des eaux du bassin du Fleuve Jaune, les rejets constants de métaux lourds et de substances radioactives finissant par contaminer les quelque 200 millions de personnes qui en dépendent pour leur approvisionnement en eau. En 2024, la Chine domine plus que jamais ce secteur stratégique, affichant une production minière de terres rares estimée à 270 000 tonnes d'oxydes[137], loin devant les États-Unis (45 000 tonnes) et l'Australie (13 000 tonnes)[138]. Ce monopole, minutieusement construit au fil des décennies, constitue un levier géopolitique d'une portée considérable, offrant à Pékin un moyen de pression sur ses concurrents industriels et technologiques. Deng Xiaoping en avait déjà perçu le potentiel dès 1992, déclarant avec lucidité : *« Le Moyen-Orient a son pétrole, la Chine a ses terres rares »*[139]. Trois décennies plus tard, cette stratégie se confirme, consolidant l'influence de l'Empire du Milieu sur les chaînes d'approvisionnement mondiales. Outre ces enjeux économiques et politiques, la concentration de l'extraction des terres rares dans des zones géographiques à risques ajoute un facteur de vulnérabilité supplémentaire : stress hydrique, menaces d'inondations et contraintes environnementales rendent ces sites particulièrement sensibles aux bouleversements climatiques, accentuant encore les défis liés à la durabilité de l'industrie numérique.

b) *Digital Labor* et renforcement des inégalités sociales

Loin de se limiter à leurs seuls effets environnementaux, les intelligences artificielles fragilisent également l'humain par leurs biais intrinsèques. Dans ce contexte, les clivages préexistants entre puissances émergentes et puissances établies se trouvent inévitablement exacerbés. Par ailleurs, les crises internes que traversent certains pays s'en trouvent aggravées. L'extraction et l'exploitation des terres rares, mais aussi des métaux alcalins et métaux de transition, nécessaires au développement des technologies numériques, alimentent ainsi de nouveaux foyers de tensions géopolitiques, à l'image de la République Démocratique du Congo (RDC), où les mines artisanales de cobalt emploient massivement des enfants. Dix ans auparavant, près de 40 000 jeunes travaillaient dans les mines de l'Est du pays, notamment dans les provinces du haut-Katanga et du Lualaba, le tout dans des conditions périlleuses avec des risques accrus d'éboulements[140]. Bien que ces coutumes aient été largement

[134] Libération. « Nucléaire : un réacteur de Three Mile Island en Pennsylvanie réactivé 45 ans après un accident radiologique." *Libération*, 20 septembre 2024. https://www.liberation.fr/international/amerique/nucleaire-un-reacteur-de-three-mile-island-en-pennsylvanie-reactive-45-ans-apres-un-accident-radiologique-20240920_D4STKGN5WRELHF6YH2H4JCXQXM/.

[135] Centre National d'Études Spatiales (CNES). « Chine - Mongolie-Intérieure : terres rares de Bayan Obo - Baotou, un enjeu technologique mondial. » *Géoimage CNES*, 2024. https://cnes.fr/geoimage/chine-mongolie-interieure-terres-rares-de-bayan-obo-baotou-un-enjeu-technologique-mondial.

[136] Les terres rares regroupent 17 éléments chimiques essentiels aux industries technologiques et énergétiques. Elles se divisent en terres rares légères (*lanthane, cérium, praséodyme, néodyme, prométhium, samarium, europium*) et terres rares lourdes (*gadolinium, terbium, dysprosium, holmium, erbium, thulium, ytterbium, lutécium, scandium, yttrium*). Leur extraction est stratégique en raison de leur usage dans les aimants, batteries et équipements de haute technologie.

[137] Unité de mesure utilisée pour quantifier la production de terres rares, correspondant à la masse des oxydes extraits de ces éléments.

[138] Statista. « Principaux pays extracteurs de terres rares dans le monde en 2024 *(en tonnes d'oxydes de terres rares)* » *Statista*, 14 Février 2025. https://fr.statista.com/statistiques/570471/principaux-pays-producteurs-de-terres-rares/.

[139] Ambassade de France en Chine, Service économique de Pékin. Analyse économique : Situation et perspectives des relations économiques franco-chinoises., « Les terres rares, une « trump card » pour la Chine dans la guerre commerciale ? », *Trésor Direction générale*, 5 septembre 2019. https://www.tresor.economie.gouv.fr/Articles/0a2d257c-e1e7-4f3f-8562-3d977e983eb5/files/a7b3092a-ed0b-4ffd-b9b5-e44175258929.

[140] Amnesty International. « République Démocratique du Congo : des enfants exploités dans les mines de cobalt, la face cachée de nos batteries. » *Amnesty International*, 2024. https://www.amnesty.fr/actualites/republique-democratique-du-congo-enfants-cobalt-face-cachee-de-nos-batterie.

réduites par des tentatives de régulations gouvernementales et des campagnes de sensibilisation, la demande croissante de cobalt ne cesse d'augmenter, passant de 104 000 tonnes en 2018, à 170 000 tonnes en 2023 (hausse de 63 %)[141]. Le cobalt est utilisé dans les semi-conducteurs pour renforcer la fiabilité des interconnexions métalliques, essentielles aux puces électroniques. Contrairement au cuivre, qui souffre de résistivité[142] accrue et d'électro migration à l'échelle nanométrique[143], le cobalt offre une meilleure stabilité thermique et une durabilité plus importante, le rendant indispensable aux technologies de pointe.

Dans le même temps, les grandes entreprises multinationales, bien qu'elles s'efforcent officiellement d'améliorer leur image, n'hésitent pas officieusement à recourir à une main-d'œuvre vulnérable dans les pays dépendants, où elles délocalisent et sous-traitent à moindre coût. Les scandales liés à ces pratiques ne manquent pas et ont, ces dernières années, largement été relayés par la presse. Le cas de Foxconn, fournisseur clé d'Apple pour l'assemblage des iPhones, illustre cette réalité. En Chine, certaines usines, notamment celle de Zhengzhou, ont été maintes fois épinglées pour leurs conditions de travail inhumaines : horaires excessifs atteignant parfois 100 heures par semaine, salaires dérisoirement bas, incompatibles avec des conditions de vie décentes, et logements précaires pour les employés. En 2019, des révélations ont montré que près de 50 % des travailleurs de cette usine étaient des intérimaires, bien au-delà du seuil légal de 10 %, mettant en lumière une exploitation systématique des plus fragiles, souvent des jeunes étudiants issus de zones rurales reculées[144]. Ces pratiques ont culminé dans des vagues de suicides à Shenzhen qui ont choqué l'opinion publique et révélé la face sombre de l'industrie technologique, notamment lorsque onze jeunes de 19 à 24 ans, se sont donné la mort depuis leurs dortoirs de travailleurs où ils vivaient entassés les uns sur les autres[145].

Par ailleurs, une enquête menée entre Paris et Antananarivo révèle que le développement de l'intelligence artificielle ne signifie pas la fin du travail lié à l'automatisation, mais plutôt son déplacement vers les pays en voie de développement. Les entreprises technologiques françaises, par exemple, externalisent les activités liées aux données vers des travailleurs situés dans des ex-colonies, notamment à Madagascar. Ces « entraîneurs » de la donnée, souvent jeunes et diplômés, sont intégrés dans un secteur plus large de services aux entreprises, allant des centres d'appels à la modération de contenu web. Malgré des contrats en CDI, la précarité demeure en raison d'une protection sociale limitée et d'une représentation syndicale faible. Ces industries, qui jouissent de zones franches, savent profiter des exonérations d'impôts et autres avantages fiscaux afin d'attirer massivement les investisseurs[146]. De même, alors que des travailleurs kenyans, payés moins de 2$ de l'heure, assurent l'entraînement de modèles d'intelligence artificielle tels que *ChatGPT*, en veillant à ce que les requêtes ne promeuvent pas de contenus discriminatoires, une forme de cynisme transparaît dans les discours universalistes dont usent les grands groupes[147].

En Afrique, si l'intelligence artificielle offre des perspectives dans des secteurs comme l'agriculture ou la santé, son adoption reste freinée par un manque d'infrastructures et de compétences numériques. Cette disparité profite aux nations et aux entreprises déjà en pointe, creusant encore davantage l'écart avec les régions moins avancées. À cela s'ajoute une menace sur

[141] BRGM. « Hausse de production de cobalt : l'Indonésie et la RDC créent un excédent d'offre sur le marché mondial. » *Mineralinfo*, 26 février 2024.https://www.mineralinfo.fr/fr/ecomine/hausse-de-production-de-cobalt-indonesie-rdc-cree-un-excedent-doffre-sur-marche-mondial.
[142] Propriété physique d'un matériau définissant son aptitude à s'opposer au passage du courant électrique. Une résistivité élevée entraîne des pertes d'énergie et une chauffe accrue dans les circuits électroniques, ce qui peut limiter les performances des semi-conducteurs.
[143] Phénomène où le courant électrique déplace progressivement les atomes d'un conducteur, provoquant une dégradation des connexions métalliques dans les puces électroniques miniaturisées. Ce phénomène est amplifié à l'échelle nanométrique, affectant la fiabilité des circuits intégrés, notamment ceux utilisant du cuivre.
[144] Le Figaro. « Apple et son sous-traitant Foxconn ont violé le droit du travail en Chine. » *Le Figaro*, 9 septembre 2019. https://www.lefigaro.fr/secteur/high-tech/apple-et-son-sous-traitant-foxconn-ont-viole-le-droit-du-travail-en-chine-20190909.
[145] Grangereau Philippe. « Suicides à la chaîne chez le géant Foxconn. » *Libération*, 3 juin 2010. https://www.liberation.fr/futurs/2010/06/03/suicides-a-la-chaine-chez-le-geant-foxconn_656243/ .
[146] Clément Le Ludec, et Maxime Cornet. « Enquête : derrière l'IA, les travailleurs précaires des pays du Sud. » *The Conversation*, 14 mars 2024. https://theconversation.com/enquete-derriere-lia-les-travailleurs-precaires-des-pays-du-sud-201503.
[147] Perrigo, Billy. "Exclusive: OpenAI Used Kenyan Workers on Less Than $2 Per Hour to Make ChatGPT Less Toxic." *Time*, 18 Janvier 2023, https://time.com/6247678/openai-chatgpt-kenya-workers/.

l'emploi : les métiers peu qualifiés, souvent répétitifs, sont progressivement remplacés par des systèmes automatisés. Le rapport de force asymétrique, tend donc à exacerber les rivalités et nourrir les luttes d'intérêt au cœur des économies du Sud Global[148]. Le renforcement des effets de la fracture numérique dans certaines zones rurales montre combien le développement technologique devient une source de rupture, le coût de la bande passante atteignant jusqu'à 44 % du PIB dans certains pays africains. En conséquence, seulement 37 % des particuliers utilisent Internet en 2023 sur le continent africain, ce qui ajoute à l'impossibilité d'accès à la donnée, et aux opportunités de développement des technologies de l'intelligence artificielle. A titre d'exemple, les trois premiers pays de la zone, leaders dans l'adoption des intelligences artificielles (l'Ile Maurice puis l'Egypte et l'Afrique du Sud), ne se hissent qu'à la 60e place au rang mondial[149].

3. IA et guerre cognitive : l'information comme arme

Loin de l'image d'une entité omnisciente et rationnelle, l'intelligence artificielle s'affirme dans le champ de la guerre cognitive comme une force chaotique, parfois insaisissable. Plutôt que d'ordonner le réel ou d'éclairer les consciences, elle agit comme un amplificateur de confusion, un catalyseur de manipulation et un verrou aux perceptions individuelles. Ses limites intrinsèques, ses biais structurels et son instrumentalisation stratégique en font un outil malléable, exploité autant pour la désinformation que pour l'ingénierie des opinions. Cette section démonte l'illusion d'une technologie infaillible, révélant comment elle nourrit la propagation d'informations biaisées, façonne les perceptions collectives et, au lieu de structurer la pensée, la fige dans des cadres idéologiques prédéterminés.

a) Désinformation et manipulation : l'IA, architecte du chaos informationnel

Les générateurs d'*infox* et les *deepfakes*, motorisés par des algorithmes avancés comme ceux développés par ClearView AI ou DeepMind, saturent de plus en plus les réseaux de récits contradictoires et offrent à leurs créateurs l'avantage de la discrétion. Les techniques de synthèses d'images dont usent à présent ces acteurs masqués, capables d'imiter et de fabriquer de toutes pièces des contenus falsifiés, représentent un sérieux problème dans la lutte informationnelle qui se joue entre grandes puissances. La guerre n'est donc plus le monopole du champ de bataille, elle continue à se propager dans le champ informationnel, polluant de manière virale les canaux de communications liant civils, décideurs politiques et soldats. Au début du conflit de l'Est en 2022, les Ukrainiens ont utilisé Clearview AI, un outil de reconnaissance faciale par intelligence artificielle, pour identifier même des corps russes défigurés, intensifiant ainsi la guerre psychologique. Cette capacité de révéler l'identité des morts en dépit de leur état, a permis à l'entreprise de redorer son image, autrefois entachée par une réputation controversée dans des cas de surveillance de masse, prouvant l'efficacité stratégique et technologique de son système dans un contexte de guerre cognitive. Jusqu'à 230 000 soldats et officiels russes ayant pris parti dans l'invasion, ont été identifiés par cet outil dans les 20 premiers mois qui ont suivis le début de la guerre[150]. Les images parfois relayées sur Télégramme, ciblant notamment des villes russes, ont participé à ébranler le moral des familles, jouant sur l'ambiguïté de l'outil afin de garder les civils dans l'incertitude sur la mort de leurs proches.

En conséquence, les opérations psychologiques (Psy-Ops) ont rapidement saisi le potentiel de cette démultiplication virale des outils de propagande générée via intelligence artificielle. Durant le mois de janvier 2024, la campagne fictive « *Come visit beautiful*

[148] Terme regroupant les pays d'Afrique, d'Amérique latine, d'Asie et d'Océanie, caractérisés par des défis de développement, des économies émergentes et une influence politique croissante sur la scène internationale. Il s'oppose aux nations industrialisées du Nord Global et reflète des dynamiques historiques, économiques et géopolitiques plutôt qu'une simple répartition géographique.
[149] Azaroual, Fahd. « L'Intelligence Artificielle en Afrique : défis et opportunités. » *Policy Center for the New South*, mai 2024. https://www.policycenter.ma/sites/default/files/2024-05/PB_23_24%20%28Azeroual%29.pdf.
[150] Bergengruen, Vera. "Ukraine's 'Secret Weapon' Against Russia Is Clearview AI." *TIME*, 12 mai 2023. https://time.com/6334176/ukraine-clearview-ai-russia/.

Gaza »[151], générée par Tel-Aviv, a parfaitement illustré cette stratégie de manipulation étatique : en moins de 48 heures, une IA générative a su concevoir des visuels idylliques de plages immaculées et de marchés animés, projetés sur Instagram auprès de milliers de comptes, occultant ainsi les destructions réelles signalées par les Nations Unies. Autre exemple frappant, le 7 octobre 2024, jour du 72e anniversaire de Vladimir Poutine, des hackers pro-ukrainiens du groupe « Sudo rm –RF » ont mené une cyberattaque massive contre les médias d'État russes. Ils ont réussi à saboter les réseaux du groupe VGTRK, interrompant la diffusion en ligne de chaînes influentes comme Russia-1 et Russia-24 pendant plusieurs heures. Dans le même temps, un *deepfake* de Vladimir Poutine a été diffusé sur la chaîne Krym24 TV en Crimée, le montrant appelant la population locale à ne pas résister aux soldats ukrainiens et affirmant l'impossibilité pour la Russie de vaincre l'armée ukrainienne[152]. Ces intrusions devenues régulières sont parfois difficiles à démasquer car elles s'appuient sur des architectures complexes : les réseaux antagonistes génératifs (GANs)[153].

Pourtant, ce déluge informationnel ne se limite pas à la sphère géopolitique. En Afrique, des fermes à trolls assistées par intelligence artificielle orchestrent des campagnes ciblées avec une précision clinique. Animées par des organisations informelles ou des ensembles de systèmes automatisés, ces entités reposent bien souvent sur l'association à des comptes fictifs et autres *bots*, dont la principale mission est de coordonner les campagnes de désinformations sur le net. Générant par vague des comptes inauthentiques qui multiplient et génèrent des interactions entre faux internautes, elles s'assurent que les publications, partages et autres commentaires amplifient les messages à visée idéologique ou politique. Un exemple concret est celui de la *Team Jorge*, entreprise clandestine montée par un ancien agent israélien spécialisé dans la manipulation électorale et la désinformation : aux côtés d'autres entités telles que *Cambridge Analytica*[154], ce groupe aurait tenté de discréditer près de 33 campagnes électorales depuis plus de 10 ans, comme durant les récentes élections kenyanes de 2022. Infiltrant les messageries de dirigeants africains et employant des plateformes numériques sophistiquées, ce groupe était en mesure de générer massivement des avatars par mélanges de données volées sur des profils réels. La base de faux comptes, une fois stockée, permettait de générer des campagnes de *bots* automatiques, répondant les uns aux autres dans des langues et des médias différents[155]. On retrouve la même logique pour la ferme à trolls russe *Internet Research Agency* basée en banlieue de Saint-Pétersbourg, qui aurait été à l'origine d'une vaste campagne d'influence ayant touché près de 126 millions d'Américains au cours de la campagne électorale de novembre à septembre 2016. En moyenne 36 000 comptes automatisés et 1,4 million de tweets générés ont réussi à polariser le débat en jouant sur les clivages sociétaux[156]. Plutôt que d'uniformiser le discours, ces opérations creusent ainsi les fractures sociopolitiques, amplifiant des tensions existantes sous couvert d'efficacité technologique.

Face à ces dérives, plusieurs régulations et cadres juridiques ont été mis en place ou sont en cours d'élaboration pour encadrer la manipulation de l'information par les outils d'intelligence artificielle. En Europe, par exemple, le Règlement Général sur la

[151] The National Public Diplomacy Directorate at the Prime Minister's Office ; הלאומי ההסברה מערך - יחד ננצח!; "Come Visit Gaza!", *Youtube*, Hasbara, 21 Janvier 2024, https://www.youtube.com/watch?v=dJaxKQrHE6U&ab_channel=%D7%9E%D7%A2%D7%A8%D7%9A%D7%94%D7%94%D7%A1%D7%91%D7%A8%D7%94%D7%94%D7%9C%D7%90%D7%95%D7%9E%D7%99-%D7%99%D7%97%D7%93%D7%A0%D7%A0%D7%A6%D7%97%21%E2%80%8F

[152] Molinari, Guillaume. « Les deepfakes au cœur de la guerre informationnelle russo-ukrainienne. » *The Conversation*, 6 juin 2023. https://theconversation.com/les-deepfakes-au-coeur-de-la-guerre-informationnelle-russo-ukrainienne-240945.

[153] Les réseaux antagonistes génératifs (GANs) sont un type d'intelligence artificielle composé de deux réseaux neuronaux : un générateur, qui crée des données artificielles (images, textes, sons), et un discriminateur, qui les évalue pour distinguer le vrai du faux. En compétition, ces réseaux permettent de produire des contenus d'une qualité et d'un réalisme croissants, utilisés notamment pour les *deepfakes*, la création artistique et la simulation de données.

[154] Cambridge Analytica était une entreprise britannique de communication stratégique spécialisée dans l'analyse de données et le micro-ciblage électoral. Elle a été impliquée dans plusieurs scandales, notamment l'exploitation illégale des données de 87 millions d'utilisateurs Facebook pour influencer des campagnes comme le Brexit en 2016 et l'élection présidentielle américaine de la même année. L'entreprise a cessé ses activités en 2018 après une controverse mondiale sur la manipulation de l'opinion publique via les réseaux sociaux.

[155] AFP, « Une ferme à trolls israélienne a influencé des dizaines d'élections en Afrique. » *VOA Afrique*, 15 février 2023. https://www.voaafrique.com/a/une-ferme-à-trolls-israélienne-a-influencé-des-dizaines-d-élections-en-afrique/6963856.html.

[156] Gérard, Colin. « Usines à trolls » russes : de l'association patriotique locale à l'entreprise globale. » *La Revue des Médias*, 20 juin 2019. https://larevuedesmedias.ina.fr/usines-trolls-russes-de-lassociation-patriotique-locale-lentreprise-globale.

Protection des Données (RGPD) offre déjà un cadre strict concernant la collecte et l'utilisation des données personnelles, même si ce texte ne vise pas directement la désinformation ; il impose toutefois des principes clés de transparence et de sécurité de traitement[157]. Par ailleurs, la mise en place du *Digital Services Act* (DSA) par l'Union Européenne depuis 2022 cherche à responsabiliser davantage les plateformes numériques en les obligeant à surveiller et à retirer rapidement les contenus mensongers ou trompeurs, tendant à les forcer à se responsabiliser. Le DSA s'applique à toutes les entreprises qui opèrent au sein de l'UE et promet des sanctions allant jusqu'à 6 % du chiffre d'affaire annuel mondial[158]. Aux États-Unis, certains États ont adopté des législations spécifiques concernant l'utilisation des *deepfakes* dans des contextes particuliers, comme la création de vidéos pornographiques non consenties ou la manipulation d'informations lors des périodes électorales. Le Texas, la Californie, le Minnesota et la Virginie sont particulièrement punitifs à cet égard, cumulant amendes élevées et peines d'emprisonnement jusqu'à un an[159]. Cependant, il n'existe pas encore de cadre réglementaire universel qui s'applique de manière homogène à la manipulation de l'information par l'intelligence artificielle dans le monde entier. Malgré les efforts, le rythme rapide des avancées technologiques complique la mise en place de régulations efficaces et universelles, rendant d'autant plus crucial le rôle des médias, des organisations de *fact-checking* et de la société civile dans la vigilance contre les dérives numériques.

b) Formatage des perceptions : une IA qui enferme plus qu'elle ne libère

Dans le champ complexe de l'ère numérique, l'intelligence artificielle ne se contente pas de façonner l'information : elle modèle également les perceptions, enfermant les individus dans des schémas prédéfinis. Ainsi, loin d'incarner une intelligence universelle, l'intelligence artificielle soulève des enjeux éthiques et politiques majeurs. Cette problématique se manifeste de manière saisissante dans divers contextes, que ce soit dans des zones de conflit ou dans des systèmes de surveillance étatiques, illustrant la manière dont la technologie, en l'absence d'un contrôle rigoureux, peut devenir un instrument discriminatoire. Prenons d'abord l'exemple de la Cisjordanie occupée où, début 2023 à Hébron, un dispositif de tir nommé *Smash*, a été mis en place aux check-points, destiné à surveiller les quelques 37 000 Palestiniens qui s'y rassemblent. Ce viseur s'installe sur des *flash-balls* pilotables à distance et est capable de « verrouiller » de façon autonome une cible reconnue suspecte via ses mouvements ou ses traits faciaux, pour ensuite, après validation de la légitimité de la cible par l'opérateur, déclencher le tir. Cet outil de neutralisation développé par l'entreprise *Smart Shooter* est non seulement capable de tirer et produire des dispersements de foules, mais il est aussi optimisé pour lancer des grenades assourdissantes et des fumigènes, selon le choix de l'opérateur, participant dès lors à une forme d'apartheid technologique où l'opérateur ne porte plus toute la responsabilité dans les manœuvres létales[160].

De même, à Jérusalem-Est, la plateforme *Red Wolf* de reconnaissance faciale a soulevé des questionnements quant aux problématiques de contrôle des déplacements et de vols d'informations personnelles destinées à nourrir une base de donnés illégitimes (*Wolf Pack),* complétée elle-même par l'application pour smartphone *Blue Wolf.* Mise en place dans les points de contrôle, cette triade est particulièrement efficace pour du relevé d'empreintes biométriques, du scan et du renseignement global sur les habitudes et l'entourage des Palestiniens. Cette ségrégation est d'autant plus forte qu'elle est accompagnée d'un vol de vie privée, une interdiction d'accès à certains secteurs, ainsi qu'un réseau de caméras de surveillance en circuit fermé (SCF) du nom de *Mabat 2000*. Actif depuis 2017, cet ensemble s'étend sur près de 10 kilomètres carrés non loin de la vieille ville et de

[157] Commission nationale de l'informatique et des libertés (CNIL). « Le règlement européen sur la protection des données (RGPD). » *CNIL*, 24 mai 2016, https://www.cnil.fr/fr/reglement-europeen-protection-donnees.
[158] Commission européenne. "The Digital Services Act." *European Commission*, 22 Octobre 2022, https://commission.europa.eu/strategy-and-policy/priorities-2019-2024/europe-fit-digital-age/digital-services-act_en.
[159] Larkin, CJ. "Regulating Election Deepfakes: A Comparison of State Laws." *Tech Policy Press*, 8 Janvier 2025, https://www.techpolicy.press/regulating-election-deepfakes-a-comparison-of-state-laws/.
[160] France Info, « *En Cisjordanie, une arme gérée par une intelligence artificielle testée à un checkpoint suscite l'inquiétude*. », 27 octobre 2022, https://www.francetvinfo.fr/replay-radio/en-direct-du-monde/en-cisjordanie-une-arme-geree-par-une-intelligence-artificielle-testee-a-un-checkpoint-suscite-l-inquietude_5579040.html.

Cheikh Jarrah, avec quasiment une caméra de reconnaissance faciale tous les cinq mètres[161]. Dans cet espace où seulement 800 colons israéliens coexistent avec des locaux, le déploiement de tels moyens parait quelque peu démesuré, s'extirpant du concept de liberté individuelle en imposant à chacun une atmosphère d'insécurité et de méfiance généralisée.

De même, le cas chinois offre une illustration particulièrement dystopique de cette dynamique, atteignant le niveau institutionnel. Depuis 2005, le système de surveillance *Skynet* s'est progressivement implanté dans le tissu urbain, pour atteindre en 2020 un déploiement de près de 626 millions de caméras, couvrant ainsi 90 % des espaces publics urbains[162]. Plus spécifiquement, dans la région du Xinjiang, l'application *IJOP (Integrated joint operation platform*) est utilisée pour collecter chaque mois des points de données sur les populations Ouïghours[163]. Cette collecte massive porte sur des informations variées dans près de 36 catégories : appels téléphoniques, déplacements, achats, usage des réseaux privés virtuels (VPN) et permet d'établir un suivi constant des comportements individuels[164]. Parallèlement, le système de crédit social chinois, mis en place entre 2014 et 2021, a sanctionné en 2018 près de 17 millions de citoyens en les empêchant de voyager par voie aérienne, en se basant sur des scores jugés insuffisants. Ce régime de notation, qui vise à échelonner entre 350 et 950 points les entreprises et les individus, agit de manière tentaculaire dans la vie des citoyens, se faisant le juge des habitudes d'achats par l'intermédiaire des réseaux de caméras positionnés dans la grande majorité des lieux publics, établissant un examen des casiers judiciaires, des données financières et fiscales ainsi que des comportements en ligne de chaque individu[165]. L'intelligence artificielle est donc partout où elle peut devenir outil d'ingénierie sociale, usant des outils de prédiction comportementale, de notation automatisée et de reconnaissance par vidéo avancée (visages et démarches).

Plus globalement, les recherches pionnières menées par Joy Buolamwini au MIT Media Lab ont mis en lumière des biais systémiques dans les algorithmes de reconnaissance faciale, révélant une discrimination structurelle dans ces technologies. Son étude, intitulée *Gender Shades*, a analysé les performances de systèmes développés par IBM, Microsoft et Face++[166], démontrant une nette disparité dans l'identification des individus en fonction de leur sexe et de leur couleur de peau. Les résultats sont clairs : alors que ces algorithmes affichent un taux de précision supérieur à 95 % pour les hommes à la peau claire, leur efficacité chute drastiquement pour les femmes à la peau foncée, avec des taux de reconnaissance pouvant descendre à 77,6 %[167]. Cette distorsion découle d'un biais de représentation dans les bases de données d'apprentissage, souvent dominées par des visages masculins et caucasiens, entraînant un effet de renforcement des inégalités technologiques. Ce phénomène s'explique par l'absence de diversité dans les bases de données utilisées pour entraîner ces modèles. Comme toute intelligence artificielle, la reconnaissance faciale repose sur un apprentissage supervisé, où l'efficacité de l'algorithme dépend directement de la représentativité des échantillons fournis. Or, lorsque ces bases de données sont déséquilibrées, les résultats produits sont biaisés,

[161] Amnesty International, "*Israeli Authorities Are Using Facial Recognition Technology to Entrench Apartheid*.", 2 mai 2023, https://www.amnesty.org/fr/latest/news/2023/05/israel-opt-israeli-authorities-are-using-facial-recognition-technology-to-entrench-apartheid/.
[162] Paul Crespo, « Surveillance high-tech en Chine : un despotisme numérique», *Bitter Winter*, 14 mars 2019, https://fr.bitterwinter.org/surveillance-high-tech-en-chine-un-despotisme-numerique/.
[163] Les Ouïghours sont un peuple turcophone et majoritairement musulman vivant principalement dans la région autonome du Xinjiang, en Chine. Minorité ethnique, ils font l'objet d'une politique de répression de la part du gouvernement chinois, incluant une surveillance massive, l'internement dans des camps de rééducation et des restrictions culturelles et religieuses, dénoncées comme des violations des droits humains par la communauté internationale.
[164] AFP. « Chine : HRW dénonce la surveillance quotidienne au Xinjiang grâce à une application », *Le Point*, 2 mai 2019, https://www.lepoint.fr/monde/chine-hrw-denonce-la-surveillance-quotidienne-au-xinjiang-grace-a-une-application-02-05-2019-2310518_24.php.
[165] Lydie Dabirand, « Système de crédit social chinois : le big data pour noter les citoyens », *Crédigo*, 10 janvier 2023, https://www.credigo.fr/actualites/systeme-credit-social-chinois-big-data-pour-noter-citoyens.html.
[166] Face++ est une plateforme de reconnaissance faciale développée par la société chinoise Megvii, spécialisée dans l'intelligence artificielle. Lancée en 2012, elle utilise des algorithmes avancés pour identifier, analyser et comparer des visages à partir d'images ou de vidéos, et est notamment employée dans la surveillance, la sécurité et les services financiers.
[167] Joy Buolamwini et Timnit Gebru. "Study finds gender and skin-type bias in artificial intelligence systems ", *MIT News*, 12 février 2018, https://news.mit.edu/2018/study-finds-gender-skin-type-bias-artificial-intelligence-systems-0212.

créant un effet de boucle rétroactive[168] : plus une population est sous-représentée, plus les erreurs se multiplient, renforçant les discriminations structurelles dans les systèmes décisionnels automatisés. Dans un cadre sécuritaire ou juridique, ces erreurs peuvent avoir des conséquences dramatiques, entraînant une surveillance infondée, des erreurs judiciaires ou encore une stigmatisation accrue sur certaines populations.

[168] Mécanisme dans les modèles d'intelligence artificielle où les résultats générés sont réintégrés dans le système pour affiner ses prédictions et améliorer ses performances. Ce processus d'apprentissage itératif permet à l'IA de s'adapter en continu aux nouvelles données et aux retours des utilisateurs.

Conclusion

Démythifier l'IA, c'est d'abord reconnaître sa nature et ses lacunes profondément humaines. Tout au long de cette étude, il a fallu déconstruire l'idée largement répandue d'une machine autonome, intelligente au sens fort, capable de remplacer l'homme. Loin des récits technologiques empreints de fantasmes, celle-ci se révèle comme un assemblage algorithmique sophistiqué, certes, mais limité par la qualité des données qui la constituent. Dépourvue d'intuition et d'une conscience, la machine reproduit simplement des schémas, restant tributaire des logiques humaines qui l'alimentent et l'emploient. Cette première partie a donc permis de remettre l'IA à sa juste place : non comme un sujet autonome, mais comme un subordonné, une prothèse, un outil parmi d'autres au service d'objectifs définis par l'homme. Dans le champ militaire, ce repositionnement s'avère particulièrement crucial. Loin de bouleverser la nature de la guerre, l'IA vient en prolonger certaines dynamiques : la recherche d'efficacité, la complexité du front, l'importance de la donnée et de la rapidité décisionnelle. Comme le souligne ainsi le chef d'état-major de l'armée de Terre (CEMAT) *« la guerre reste ce qu'elle est : un affrontement humain »,* bien qu'elle *« soulève des questions d'ordre polémologique et anthropologique qui interrogent la place même de l'homme dans la guerre. »*[169]. Il ne s'agit donc pas de déléguer le conflit aux machines, mais de mieux outiller la prise de décision et l'action. L'IA peut apporter des gains concrets dans la fiabilisation et l'accélération des boucles décisionnelles, ou encore dans l'optimisation du potentiel individuel du soldat, mais ces progrès techniques doivent être interprétés avec prudence. D'autant plus que les terrains d'expérimentation récents, du Donbass à Gaza, montrent combien les promesses de rationalisation ou de précision sont souvent contredites par la friction du réel et la volatilité des contextes.

Pour autant, l'intégration de l'intelligence artificielle dans les processus de défense n'est pas une option stratégique, mais bien une nécessité géopolitique et opérationnelle. À l'heure où les grandes puissances investissent massivement dans la guerre algorithmique, où des adversaires technologiquement avancés exploitent le levier de la guerre cognitive, refuser l'IA reviendrait à s'auto-marginaliser. Là encore, le Général Pierre Schill l'exprime avec clarté : *« si s'approprier l'IA ne garantira pas nos succès à venir, omettre de le faire garantira d'emblée un déclassement dans les combats de demain*[170]*».* Maintenir l'initiative sur le champ de bataille passe donc par une maîtrise technologique qui ne doit rien au mimétisme, mais tout à une stratégie nationale fondée sur la souveraineté numérique, la simplification des outils et l'adaptabilité doctrinale. Porté par la France au récent sommet qu'elle a accueilli sur son sol, le développement d'une IA souveraine et fiable, simple d'emploi, capable de soutenir les forces sans s'imposer à elles, se fait plus que pressant. Mais intégrer ces systèmes ne signifie pas les sanctuariser. La dernière partie de cette étude a précisément mis en évidence les fragilités d'un déploiement non encadré : dépendance aux données, risque d'asymétrie, pollution algorithmique, perte de lisibilité stratégique. Face à ces risques, la prudence reste un impératif. Le Général Schill nous rappelle donc que *« comme pour toute révolution capacitaire, il s'agit de ne pas céder aux sirènes du tout technologique »*[171]. L'IA doit rester un levier, non un pilote. Elle peut accroître notre agilité, mais ne saurait nous dispenser de penser. L'innovation, dans le domaine militaire comme ailleurs, ne peut se substituer à la stratégie, encore moins à l'éthique. Démythifier l'IA, c'est donc rappeler qu'elle ne saurait être une fin en soi. C'est refuser la fascination naïve pour les outils, tout en assumant les responsabilités qui incombent à leur usage. En somme, l'IA ne sera jamais l'acteur du combat ; elle en sera, au mieux, le facilitateur. Et c'est justement dans ce rôle second qu'elle peut devenir un atout, à condition de ne jamais confondre l'outil et le stratège.

[169] Laurent Lagneau, *« Pour le général Schill, l'intelligence artificielle ne changera pas la nature de la guerre »*, Opex360, 14 janvier 2024, www.opex360.com/2024/01/14/pour-le-general-schill-lintelligence-artificielle-ne-changera-pas-la-nature-de-la-guerre/.
[170] Laurent Lagneau, *« Pour le général Schill, l'intelligence artificielle ne changera pas la nature de la guerre »*, Opex360, 14 janvier 2024, www.opex360.com/2024/01/14/pour-le-general-schill-lintelligence-artificielle-ne-changera-pas-la-nature-de-la-guerre/.
[171] *Section technique de l'armée de Terre (STAT)*, « Robots tueurs : des armes aux mains de l'IA ? », LinkedIn, 6 mars 2024, www.linkedin.com/posts/section-technique-de-l-arm%C3%A9e-de-terre-stat_robots-tueurs-des-armes-aux-mains-de-lia-activity-7150929912982339584-x2c9/.

Bibliographie

Commission européenne, « Proposition de règlement établissant des règles harmonisées sur l'intelligence artificielle (Artificial Intelligence Act) », COM/2021/206 final, 21 avril 2021, https://eur-lex.europa.eu/legal-content/FR/TXT/?uri=CELEX%3A52021PC0206.

Encyclopædia Britannica, « Analytical Engine », Encyclopædia Britannica Online, https://www.britannica.com/technology/Analytical-Engine.

Stanford Encyclopedia of Philosophy, « Artificial Intelligence », Stanford University, https://plato.stanford.edu/entries/artificial-intelligence/.

Aurélie Jean. (2024, 23 octobre). IA : Mythes à déconstruire, réalités à saisir - Keynote d'Aurélie Jean [Vidéo]. YouTube, https://www.youtube.com/watch?v=WSTcrL6ujsY.

Jürgen Schmidhuber, « Deep learning in neural networks: An overview », Neural Networks 61 (2015) 85–117: https://www.sciencedirect.com/science/article/abs/pii/S0893608014002135.

Krakowski, I., Kim, J., Cai, Z.R. et al. « Human-AI interaction in skin cancer diagnosis: a systematic review and meta-analysis". npj Digit. Med. 7, 78, (2024). https://doi.org/10.1038/s41746-024-01031-w

Courrier International, « Le chiffre du jour : les géants de la tech prévoient un investissement record dans l'IA en 2025 »: https://www.courrierinternational.com/article/le-chiffre-du-jour-les-geants-de-la-tech-prevoient-un-investissement-record-dans-l-ia-en-2025_227476

Le Monde, « Elon Musk et des centaines d'experts réclament une pause dans le développement de l'IA », 29 mars 2023, https://www.lemonde.fr/economie/article/2023/03/29/elon-musk-et-des-centaines-d-experts-reclament-une-pause-dans-le-developpement-de-l-ia_6167461_3234.html.

Sternberg Robert J. La théorie triarchique de l'intelligence. In: L'Orientation scolaire et professionnelle, volume 23e numéro 1, Mars 1994. Numéro spécial : Les techniques psychologiques d'évaluation des personnes. pp. 119-136. https://www.persee.fr/doc/binop_0249-6739_1994_num_23_1_1477

War on the Rocks, « A Game Changing Third Offset Strategy »: https://warontherocks.com/2014/11/a-game-changing-third-offset-strategy/

La Tribune, « La Chine désormais numéro un sur les brevets d'IA générative devant les États-Unis »: https://www.latribune.fr/technos-medias/informatique/la-chine-desormais-numero-un-sur-les-brevets-d-ia-generative-devant-les-etats-unis-1001375.html

Asia Pacific Foundation of Canada, « La rivalité entre la Chine et les États-Unis marque le »: https://www.asiapacific.ca/fr/publication/la-rivalite-entre-la-chine-et-les-etats-unis-marque-le

U.S. Department of Defense, « DOD Chief Digital and Artificial Intelligence Office Hosts Global Information Dominance » : https://www.defense.gov/News/Releases/Release/Article/3282376/dod-chief-digital-and-artificial-intelligence-office-hosts-global-information-d/

U.S. Department of Defense, « DOD Announces Project Maven ». (Publié en avril 2017) : https://www.defense.gov/News/Releases/Release/Article/1024826/dod-announces-project-maven/

NIDS (National Institute for Defense Studies – Japon), « Commentary – PDF » : https://www.nids.mod.go.jp/english/publication/commentary/pdf/commentary105e.pdf

NIDS (National Institute for Defense Studies – Japon), Publication « Security – 05 janvier 2022 » : https://www.nids.mod.go.jp/english/publication/security/pdf/2022/01/05.pdf

Covea Finance, « Principales orientations du 14ème plan quinquennal chinois » : https://particulier.covea-finance.fr/decryptages/le-point-de-vue-de-lexpert/principales-orientations-du-14eme-plan-quinquennal-chinois

Capital, « Des employés de Huawei ont collaboré avec l'armée chinoise sur des projets de recherche » : https://www.capital.fr/entreprises-marches/des-employes-de-huawei-ont-collabore-avec-larmee-chinoise-sur-des-projets-de-recherche-1343156

ZDNet, « Ernie Bot 40 plus fort que ChatGPT : c'est-ce qu'affirment ses créateurs » : https://www.zdnet.fr/actualites/ernie-bot-40-plus-fort-que-chatgpt-c-est-ce-qu-affirment-ses-createurs-39961904.htm

Araya, D., & He, A. (2024). Chinese Military Applications of AI. In United States-China Multilateralism in the Age of Military AI (pp. 8–10). Centre for International Governance Innovation. http://www.jstor.org/stable/resrep65247.12

CNN, « China Zhuhai Airshow: New Weapons » : https://edition.cnn.com/2024/11/19/china/china-zhuhai-airshow-new-weapons-intl-hnk/index.html

Amicale Nationale des Transmissions Aéroportées, « Unité 8200 : La sentinelle furtive d'Israël », Amicale Nationale des Transmissions Aéroportées, 2 avril 2024, https://amicalenationaledestransmissionsaeroportees.fr/2024/04/02/unite-8200-la-sentinelle-furtive-disrael/.

Florian Gouthière et Alexandre Horn, « Comment l'armée israélienne utilise l'intelligence artificielle pour bombarder Gaza », Libération, 2 décembre 2023, https://www.liberation.fr/checknews/comment-larmee-israelienne-utilise-lintelligence-artificielle-pour-bombarder-gaza-20231202_EMALLXEUEJB7HFEZZPM7XXZBMQ/.

Yuval Abraham, Oren Ziv, Meron Rapoport et Areej Hazboun, « 'Lavender': The AI Machine Directing Israel's Bombing Spree in Gaza », +972 Magazine, 3 avril 2024, https://www.972mag.com/lavender-ai-israeli-army-gaza/.

Laure de Roucy-Rochegonde et Amélie Ferey, « L'IA au cœur de la stratégie israélienne à Gaza », Institut français des relations internationales (IFRI), 26 février 2025, https://www.ifri.org/fr/presse-contenus-repris-sur-le-site/lia-au-coeur-de-la-strategie-israelienne-gaza.

Times for Palestine, « Unit 8200 Role in the Ongoing AI War », Times for Palestine, 10 December 2024, https://timesforpalestine.com/unit-8200-role-in-the-ongoing-ai-war/.

Israel Aerospace Industries (IAI), « ELI-4030 Drone Guard », Israel Aerospace Industries (IAI), 26 janvier 2020, https://www.iai.co.il/p/eli-4030-drone-guard.

Emmanuel Grynszpan, « Mykhailo Fedorov, ministre ukrainien : "La guerre asymétrique consiste à utiliser des technologies auxquelles l'ennemi ne s'attend pas" », Le Monde, 10 août 2024, https://www.lemonde.fr/international/article/2024/08/10/mykhailo-fedorov-ministre-ukrainien-la-guerre-asymetrique-consiste-a-utiliser-des-technologies-auxquelles-l-ennemi-ne-s-attend-pas_6275112_3210.html.

Agathe Mahuet, « Armée et IA : l'Ukraine est devenu un laboratoire pour ces nouvelles armes intelligentes qui inquiètent l'ONU », Franceinfo, 16 avril 2024, https://www.francetvinfo.fr/replay-radio/le-club-des-correspondants/armee-et-ia-l-ukraine-est-devenu-un-laboratoire-pour-ces-nouvelles-armes-intelligentes-qui-inquietent-l-onu_6453404.html.

Thierry Berthier et Yannick Harrel, « La stratégie russe de développement de l'intelligence artificielle », The Conversation, 26 novembre 2019, https://theconversation.com/la-strategie-russe-de-developpement-de-lintelligence-artificielle-127457.

Anna Nadibaidze, « La guerre low-tech de la Russie contre l'Ukraine », Le Rubicon, 3 mars 2023, https://lerubicon.org/la-guerre-low-tech-de-la-russie-contre-lukraine/.

Gregory C. Allen, « Russia Probably Has Not Used AI-Enabled Weapons in Ukraine—But That Could Change », Center for Strategic and International Studies (CSIS), 26 mai 2022, https://www.csis.org/analysis/russia-probably-has-not-used-ai-enabled-weapons-ukraine-could-change.

Fabrice Wolf, « Geran-2 : la défense ukrainienne face à l'adaptation russe », Meta-Defense, 28 novembre 2024, https://meta-defense.fr/fi/2024/11/28/geran-2-defense-ukrainne-asaptation-ru/.

Hugo Brogli et Lou Rochambeau, « Intelligence artificielle et drones autonomes : une transformation des stratégies militaires modernes ? », Portail de l'IE, 15 janvier 2025, https://www.portail-ie.fr/univers/blockchain-data-et-ia/2025/intelligence-artificielle-et-drones-autonomes-une-transformation-des-strategies-militaires-modernes/.

« Russia Manufactures Wooded Drones for Reconnaissance and Ukraine's Air Defense Distraction », Defense Express, 5 mai 2023,https://en.defenceua.com/weapon_and_tech/russia_manufactures_wooded_drones_for_reconnaissance_and_ukraines_air_defense_distraction-6612.html.

« Guerre en Ukraine, les drones gagnent leurs galons », Cerbair, 8 octobre 2024, https://www.cerbair.com/articles/guerre-en-ukraine-les-drones-gagnent-leurs-galons.

« Breaking down the Levels of Drone Autonomy », CloudFactory, 23 novembre 2021, https://www.cloudfactory.com/blog/levels-of-drone-autonomy

David Hambling, « Russian Loitering Munition Racks up Kills but Shows Limitations », Forbes, 1er décembre 2022, https://www.forbes.com/sites/davidhambling/2022/12/01/russian-loitering-munition-racks-up-kills-but-shows-limitations/?sh=408f3a225d58.

« Ukrainian Forces Get an AI-Powered Saker Scout Drone, and Its Algorithms Can Solve an Important Problem », Defense Express, 4 septembre2023, https://en.defenceua.com/weapon_and_tech/ukrainian_forces_get_an_ai_powered_saker_scout_drone_and_its_algorithms_can_solve_an_important_problem-7842.html.

Raido Saremat, "Punching above Your Weight with the Use of Modern Technology", Vegvisir Blog, 2024, https://www.vegvisir.ee/blog/punching-above-your-weight-with-the-use-of-modern-technology.

Ministère des Armées, TaiDX l'IA de défense, YouTube, 17 juin 2024, extrait à 30 min, Bertrand Rondepierre : « Système Rora », https://www.youtube.com/watch?v=6luGTTYeCS8.

Comité d'éthique de la défense, Avis sur l'usage des technologies d'intelligence artificielle par les forces armées, ministère des Armées, 14 janvier 2025, p. 13, section « L'aide à la décision, voire la décision pour la planification », https://www.defense.gouv.fr/sites/default/files/ministere-armees/20250114_np_comedef_avis-sur-l%27usage-des-technologies-d%27intelligence-artificielle-par-les-forces-armees.pdf.

Agence de l'innovation de défense, 2 projets retenus dans le cadre de l'appel à projets d'Intelligence Artificielle 2020-2021, Ministère des Armées,1er mars 2021, https://www.defense.gouv.fr/aid/actualites/2-projets-retenus-cadre-lappel-a-projets-dintelligence-artificielle-2020-2021.

Mars Attaque. « Innovation et défi du C2IA : Vers un commandement augmenté par l'intelligence artificielle. » Mars Attaque, 15 mars 2020. https://mars-attaque.blogspot.com/2020/03/innovation-defi-c2ia-commandement-cpoia-intelligence-artificielle.html.

Laurent Lagneau, Selon le Sénat, les divergences avec Berlin font douter de l'avenir du Système de combat aérien du futur, Zone Militaire - Opex360, 1er décembre 2024, https://www.opex360.com/2024/12/01/selon-le-senat-les-divergences-avec-berlin-font-douter-de-lavenir-du-systeme-de-combat-aerien-du-futur/.

Spc. Jackson Gray, Project Convergence Capstone 4 works to integrate joint, multinational defense systems, U.S. Army, 27 février 2024, https://www.army.mil/article/274045/project_convergence_capstone_4_works_to_integrate_joint_multinational_defense_systems.

Gouvernement du Canada, RDDC participe à l'expérience multinationale Projet Convergence Capstone 4, 15 novembre 2024, https://science.gc.ca/site/science/fr/blogues/science-pour-defense-securite/rddc-participe-lexperience-multinationale-projet-convergence-capstone-4.

Ministère des Armées, Rapport de la Task Force IA, septembre 2019, section « 2.1 Un cadre éthique et juridique robuste pour le ministère des Armées », p. 9, https://www.defense.gouv.fr/sites/default/files/aid/20200108-NP-Rapport%20de%20la%20Task%20Force%20IA%20Septembre.pdf.

U.S. Department of Defense, DoD Directive 3000.09: Autonomy in Weapon Systems, 25 janvier 2023, https://www.esd.whs.mil/portals/54/documents/dd/issuances/dodd/300009p.pdf.

Benoit, Marie-Claude. « La Direction générale de l'armement attribue la réalisation de la plateforme ARTEMIS.IA à ATHEA. » Actuia, 19 juillet 2022. https://www.actuia.com/actualite/la-direction-generale-de-larmement-attribue-la-realisation-de-la-plateforme-artemis-ia-a-athea/#artemisia.

Arnaud. « Les drones MQ-9 Reaper atteignent 40 000 heures de vol au Sahel. » Avions Légendaires, 6 avril 2021. https://www.avionslegendaires.net/2021/04/actu/les-drones-mq-9-reaper-atteignent-40000-heures-de-vol-au-sahel/.

Fan, Ning, Zhu Mengying and Zhang Qiang. 2021. "远超阿尔法狗？'战远'成战远远助决策 '最强大远'" [Far more than Alpha Dog? "War Skull" becomes the "strongest brain" to assist decision-making on the battlefield]. 科技日报 [Science and Technology Daily], April 19. http://digitalpaper.stdaily.com/http_www.kjrb.com/kjrb/html/2021-04/19/content_466128.htm?div=-1.

Julien Lausson, « La Russie est suspectée d'avoir largement brouillé les GPS en Pologne, » Numerama, 18 janvier 2024, https://www.numerama.com/cyberguerre/1612064-la-russie-est-suspectee-davoir-largement-brouille-les-gps-en-pologne.html.

Thales. « Modem 21 et sécurisation des communications militaires par satellites : une innovation majeure. » Thales, 13 septembre 2023. https://www.thalesgroup.com/fr/monde/defense/news/modem-21-et-securisation-des-communications-militaires-satellites-une-innovation.

Georges Lagueyrie. « Les 'Dragon Drones', ces nouveaux engins volants lance-flammes que les Ukrainiens utilisent face aux Russes. » Le Figaro, 11 septembre 2024. https://www.lefigaro.fr/international/les-dragon-drones-ces-nouveaux-engins-volants-lance-flammes-que-les-ukrainiens-utilisent-face-aux-russes-20240911.

Nations Unies. « L'ONU adopte une résolution historique pour réglementer l'intelligence artificielle. » Nouvelles ONU, 21 mars 2024. https://news.un.org/fr/story/2024/03/1144211.

Institut Montaigne. « Quantique : vers une logique de marché » – Résumé. Institut Montaigne, Octobre 2024. https://www.institutmontaigne.org/ressources/pdfs/publications/resume-quantique-vers-une-logique-de-marche.pdf.

Ministère des Armées. « Lancement du programme Proqcima et notification d'accords-cadres pour le développement d'ordinateurs quantiques universels. » Ministère des Armées, 6 mars 2024. https://www.defense.gouv.fr/sites/default/files/ministerearmees/06.03.2024%20Lancement%20du%20programme%20Proqcima%20et%20notification%20d%E2%80%99accordscadres%20pour%20le%20d%C3%A9veloppement%20d%E2%80%99ordinateurs%20quantiques%20universels.pdf.

Ministère de la Transition écologique. "Intelligence artificielle durable." Ministère de la Transition écologique, 10 février 2025. https://www.ecologie.gouv.fr/actualites/intelligence-artificielle-durable.

Commission européenne. "AI and Generative AI: Transforming Europe's Electricity Grid for a Sustainable Future." Digital Strategy, 22 février 2025. https://digital-strategy.ec.europa.eu/fr/library/ai-and-generative-ai-transforming-europes-electricity-grid-sustainable-future.

Agence France-Presse. « L'AIE va lancer un observatoire sur l'impact de l'IA sur la consommation d'énergie. » Connaissance des Énergies, 11 février 2025. https://www.connaissancedesenergies.org/afp/laie-va-lancer-un-observatoire-sur-limpact-de-lia-sur-la-consommation-denergie-250211.

Libération. « Nucléaire : un réacteur de Three Mile Island en Pennsylvanie réactivé 45 ans après un accident radiologique." Libération, 20 septembre 2024. https://www.liberation.fr/international/amerique/nucleaire-un-reacteur-de-three-mile-island-en-pennsylvanie-reactive-45-ans-apres-un-accident-radiologique-20240920_D4STKGN5WRELHF6YH2H4JCXQXM/.

Centre National d'Études Spatiales (CNES). « Chine - Mongolie-Intérieure : terres rares de Bayan Obo - Baotou, un enjeu technologique mondial. » Géoimage CNES, 2024. https://cnes.fr/geoimage/chine-mongolie-interieure-terres-rares-de-bayan-obo-baotou-un-enjeu-technologique-mondial.

Statista. « Principaux pays extracteurs de terres rares dans le monde en 2024 (en tonnes d'oxydes de terres rares) » Statista, 14 Février 2025. https://fr.statista.com/statistiques/570471/principaux-pays-producteurs-de-terres-rares/.

Ambassade de France en Chine, Service économique de Pékin. Analyse économique : Situation et perspectives des relations économiques franco-chinoises., « Les terres rares, une « trump card » pour la Chine dans la guerre commerciale ? », Trésor Direction générale, 5 septembre 2019. https://www.tresor.economie.gouv.fr/Articles/0a2d257c-e1e7-4f3f-8562-3d977e983eb5/files/a7b3092a-ed0b-4ffd-b9b5-e44175258929.

Amnesty International. « République Démocratique du Congo : des enfants exploités dans les mines de cobalt, la face cachée de nos batteries. » Amnesty International, 2024. https://www.amnesty.fr/actualites/republique-democratique-du-congo-enfants-cobalt-face-cachee-de-nos-batterie.

BRGM. « Hausse de production de cobalt : l'Indonésie et la RDC créent un excédent d'offre sur le marché mondial. » Mineralinfo, 26 février 2024, https://www.mineralinfo.fr/fr/ecomine/hausse-de-production-de-cobalt-indonesie-rdc-cree-un-excedent-doffre-sur-marche-mondial.

Le Figaro. « Apple et son sous-traitant Foxconn ont violé le droit du travail en Chine. » Le Figaro, 9 septembre 2019. https://www.lefigaro.fr/secteur/high-tech/apple-et-son-sous-traitant-foxconn-ont-viole-le-droit-du-travail-en-chine-20190909.

Clément Le Ludec, et Maxime Cornet. « Enquête : derrière l'IA, les travailleurs précaires des pays du Sud. » The Conversation, 14 mars 2024. https://theconversation.com/enquete-derriere-lia-les-travailleurs-precaires-des-pays-du-sud-201503.

Botero Castro, María Camila, Francisca López Molina, et Johan Alexander Sanabria Restrepo. « Les êtres humains cachés derrière l'IA en Amérique latine. » Global Voices, 30 septembre 2024. https://fr.globalvoices.org/2024/09/30/290760/.

Azaroual, Fahd. « L'Intelligence Artificielle en Afrique : défis et opportunités. » Policy Center for the New South, mai 2024. https://www.policycenter.ma/sites/default/files/2024-05/PB_23_24%20%28Azeroual%29.pdf.

Bergengruen, Vera. "Ukraine's 'Secret Weapon' Against Russia Is Clearview AI." TIME, 12 mai 2023. https://time.com/6334176/ukraine-clearview-ai-russia/.

The National Public Diplomacy Directorate at the Prime Minister's Office ; הלאומי ההסברה מערך - יחד ננצח!; "Come Visit Gaza!", Youtube, Hasbara, 21 Janvier 2024, https://www.youtube.com/watch?v=dJaxKQrHE6U&ab_channel=%D7%9E%D7%A2%D7%A8%D7%9A%D7%94%D7%94%D7%A1%D7%91%D7%A8%D7%94%D7%94%D7%9C%D7%90%D7%95%D7%9E%D7%99-%D7%99%D7%97%D7%93%D7%A0%D7%A0%D7%A6%D7%97%21%E2%80%8F.

Molinari, Guillaume. « Les deepfakes au cœur de la guerre informationnelle russo-ukrainienne. » The Conversation, 6 juin 2023. https://theconversation.com/les-deepfakes-au-coeur-de-la-guerre-informationnelle-russo-ukrainienne-240945.

AFP, « Une ferme à trolls israélienne a influencé des dizaines d'élections en Afrique. » VOA Afrique, 15 février 2023. https://www.voaafrique.com/a/une-ferme-à-trolls-israélienne-a-influencé-des-dizaines-d-élections-en-afrique/6963856.html.

Gérard, Colin. « Usines à trolls » russes : de l'association patriotique locale à l'entreprise globale. » La Revue des Médias, 20 juin 2019. https://larevuedesmedias.ina.fr/usines-trolls-russes-de-lassociation-patriotique-locale-lentreprise-globale.

Commission nationale de l'informatique et des libertés (CNIL). « Le règlement européen sur la protection des données (RGPD). » CNIL, 24 mai 2016, https://www.cnil.fr/fr/reglement-europeen-protection-donnees.

Commission européenne. "The Digital Services Act." European Commission, 22 Octobre 2022, https://commission.europa.eu/strategy-and-policy/priorities-2019-2024/europe-fit-digital-age/digital-services-act_en.

France Info, « En Cisjordanie, une arme gérée par une intelligence artificielle testée à un checkpoint suscite l'inquiétude. », 27 octobre 2022, https://www.francetvinfo.fr/replay-radio/en-direct-du-monde/en-cisjordanie-une-arme-geree-par-une-intelligence-artificielle-testee-a-un-checkpoint-suscite-l-inquietude_5579040.html.

Amnesty International, "Israeli Authorities Are Using Facial Recognition Technology to Entrench Apartheid.", 2 mai 2023, https://www.amnesty.org/fr/latest/news/2023/05/israel-opt-israeli-authorities-are-using-facial-recognition-technology-to-entrench-apartheid/.

Paul Crespo, « Surveillance high-tech en Chine : un despotisme numérique», Bitter Winter, 14 mars 2019, https://fr.bitterwinter.org/surveillance-high-tech-en-chine-un-despotisme-numerique/.

AFP. « Chine : HRW dénonce la surveillance quotidienne au Xinjiang grâce à une application », Le Point, 2 mai 2019, https://www.lepoint.fr/monde/chine-hrw-denonce-la-surveillance-quotidienne-au-xinjiang-grace-a-une-application-02-05-2019-2310518_24.php.

Lydie Dabirand, « Système de crédit social chinois : le big data pour noter les citoyens », Crédigo, 10 janvier 2023, https://www.credigo.fr/actualites/systeme-credit-social-chinois-big-data-pour-noter-citoyens.html.

Joy Buolamwini et Timnit Gebru. "Study finds gender and skin-type bias in artificial intelligence systems ", MIT News, 12 février 2018, https://news.mit.edu/2018/study-finds-gender-skin-type-bias-artificial-intelligence-systems-0212.

Laurent Lagneau, « L'Armée de Terre mise sur l'intelligence artificielle pour élaborer des décisions opérationnelles tactiques », Zone Militaire - Opex360, 17 avril 2024, https://www.opex360.com/2024/04/17/larmee-de-terre-mise-sur-lintelligence-artificielle-pour-elaborer-des-decisions-operationnelles-tactiques/.

Internet

@CombatsFuturs
@CombatsFuturs
@Commandement du combat futur
www.terre.defense.gouv.fr/ccf

Intranet

https://deftube.intradef.gouv.fr/channels/#ccf
https://portails-federateurs.intradef.gouv.fr/ccf/

Comité de rédaction : CEST/BOC

Rédacteurs : Mlle Charline GEAY, CBA Karim LOUARDI.

Commandement du combat futur
1, place Joffre – Case 53
75007 Paris SP 07