

L'intelligence artificielle militaire : du rêve au glaive

Louis Perez | 25 mai 2023 | ARTICLES | 



L'intelligence artificielle (IA) fait l'objet de débats mouvementés entre les partisans, idéalistes ou anxieux, d'une révolution technologique qui serait en voie de transformer le monde et ceux, plus sceptiques, qui ne voient là qu'une mode technologique dopée par un marketing basé sur des interrogations existentialistes. Ces débats sont illustrés par l'application Chat GPT dont les performances ne cessent [d'étonner](#) ou [d'effrayer](#). La sphère militaire, où certains [appellent](#) d'ailleurs à un usage de Chat GPT, ne reste naturellement pas indifférente à l'IA tant les avancées technologiques peuvent être décisives dans la guerre. L'intelligence artificielle (IA) dans la guerre est déjà une réalité. En 2021, l'armée israélienne [affirmait](#) ainsi conduire la première guerre de l'IA. Depuis 2022, la situation en Ukraine représente le premier conflit majeur entre puissances disposant de moyens technologiques avancés, propres ou tiers, où se déploient des systèmes d'IA (SIA). Alors que les États accumulent des documents stratégiques militaires sur la façon dont ils développeront et utiliseront l'IA à court et moyen termes, on peut s'interroger sur ce qui relève, d'une part, d'une [communication technologique militaire](#), voire d'un [solutionnisme](#) naïf et, d'autre part, des réalités stratégiques et opérationnelles. Cette contribution interrogera par conséquent la réalité de cette technologie, à travers sa conceptualisation et son histoire, et de ses apports militaires, au regard du terrain ukrainien.

Définition : cerner les contours de l'IA

Une première difficulté qui accompagne l'appréhension de l'IA militaire (IAM) réside la définition même de l'IA : il n'existe pas de définition consensuelle. Si l'on arrive rarement à une acception claire et unanime d'un domaine scientifique, on parvient cependant à circonscrire son étendue et sa raison d'être, ce qui n'est pas nécessairement le cas avec l'IA. Les doutes autour de l'IA renvoient aux deux mots mêmes qui forment cette expression apparue pour la [première fois](#) en 1956 lors d'une conférence à l'Université de Dartmouth. En effet, si l'on éprouve des difficultés à définir l'IA, c'est d'abord parce qu'il n'y a [pas de définition précise](#) de l'intelligence. L'utilisation du terme « intelligence » importe une charge anthropomorphique qui s'est répandue dans le domaine (apprentissage automatique, réseaux de neurones, autonomie). Ces éléments poussent à assimiler les SIA à l'humain

et opèrent un lien problématique entre science et science-fiction sur lequel nous reviendrons. Le qualificatif « [artificiel](#) » évoque pour sa part sa dimension scientifique. À cet égard, il n'est pas toujours évident de déceler le périmètre scientifique de l'IA, souvent taxée de [fourre-tout technologique](#). Il en résulte un objet évanescant qui s'illustre par l'« [effet IA](#) » selon lequel l'IA serait ce qui n'a pas encore été fait en matière de délégation de tâches à une machine.

Les incertitudes quant à ce que revêt l'IA ont été résumées par le chercheur Eliezer Yudkowsky qui [conclut](#) que « *By far the greatest danger of Artificial Intelligence is that people conclude too early that they understand it.* ». D'aucuns ont dès lors proposé [d'abandonner](#) l'utilisation de la dénomination « IA » au profit d'expressions plus précises et moins litigieuses (apprentissage automatique, informatique cognitive, etc.). Mais la société s'est saisie de l'expression et les décideurs publics en ont fait un objet et un usage politiques. Réfléchir à une meilleure dénomination fait partie du débat, mais cela ne peut éluder les nécessités d'étudier ce qui se cache derrière. Il est dès lors nécessaire de se prêter à un effort de rationalisation de la notion.

Il faut en réalité distinguer deux dimensions lorsque le terme IA est employé : mythique et scientifique. Au demeurant, le mythe et la science poursuivent le même but, celui d'expliquer les phénomènes, mais emploient des méthodes de vérification bien différentes. À partir des philosophes présocratiques, la trajectoire de la connaissance n'a cessé de réduire la part du mythe – qui demeure malgré tout – au profit de la science. Ainsi, l'IA comporte une incontournable dimension mythique. Que ce soit Galatée, la statue de Pygmalion animée par Aphrodite, la créature du Docteur Frankenstein ou HAL3000 dans *2001 l'Odyssée de l'espace*, le mythe d'un être doté d'une intelligence non naturelle a toujours existé. Si les raisons et les modalités de ces mythes ont varié, ils renferment toujours une dimension existentielle, répondre aux appréhensions de l'homme (origine de la vie, dépassement technologique), ainsi qu'une dimension fonctionnelle, servir ses besoins. À l'ère contemporaine, le [désenchantement du monde](#) n'a pas terni l'approche mythique de l'IA. Science et science-fiction s'influencent mutuellement, mais lorsque l'on appréhende l'IA il faut garder à l'esprit les limites de chacun. Face aux [cris d'alarme](#) récurrents sur l'avènement d'une super-IA, aux capacités surhumaines et aux velléités eschatologiques, il convient de garder raison, attitude d'ailleurs propre à la science. Pour ce faire, il est nécessaire de revenir sur le projet scientifique de l'IA.

L'intelligence artificielle comme domaine de recherche émerge à la moitié du XXe siècle. Mais l'étude de la logique et du raisonnement formels remonte à l'Antiquité, par exemple chez Aristote ou Euclide, et s'est prolongée chez les philosophes modernes comme Pascal ou Hobbes qui [affirme](#) dans le *Léviathan* que « la raison n'est rien d'autre que calculs ». L'IA n'est pas une science à part entière, mais un domaine ou une sous-discipline scientifique qui puise ses ressources au sein de plusieurs disciplines scientifiques. Sommairement, les travaux actuels en IA sont essentiellement le fruit d'une concentration des recherches en mathématiques et en informatique. Si elle dépend d'autres disciplines, l'IA a son propre champ scientifique qui se caractérise par un objectif propre (la reproduction de fonctions associées à l'intelligence afin d'assister les humains), des méthodes spécifiques (algorithmes connexionnistes ou symboliques) et une communauté scientifique singulière. L'articulation entre mythe et science aborde l'IA sous l'angle disciplinaire, mais en réalité c'est bien souvent les SIA, le produit du domaine scientifique, qui font l'objet des discussions.

Les SIA sont essentiellement des outils de traitement de données qui mettent en lumière des corrélations pour des objectifs variés (classification, détection, modélisation, simulation, personnalisation, optimisation, prévision). En ce sens, les SIA sont parfois qualifiés de technologie générique ou polyvalente, car ils peuvent servir de nombreux objectifs dans des domaines divers, même si les tâches demeurent très précises. Ils peuvent en outre être intégrés et connectés avec d'autres systèmes, notamment robotiques afin de faciliter par exemple des fonctions de navigation. À ce titre, les SIA entretiennent des liens étroits avec la notion polysémique d'autonomie. Comme pour l'IA, le terme d'autonomie est utilisé de façon différente par les acteurs concernés. Soit, cela renvoie au degré d'intervention humaine face à des fonctions automatiques programmées. Soit, cela soulève l'idée d'une indépendance des SIA par rapport à l'homme. Le premier cas relève de la science et de la technique, le second du mythe. Il convient donc de se garder du spectre du *Terminator* qui sert souvent à détourner l'attention des enjeux que représentent les SIA actuels.

En ces quelques lignes nous avons donc retracé une possible définition de l'IA : un domaine de recherche interdisciplinaire visant à développer des systèmes algorithmiques informatiques qui, par le biais de caractéristiques techniques, peuvent réaliser et mettre en œuvre des fonctions précises, similaires ou supérieures aux capacités intellectuelles associées aux êtres humains afin d'assister ces derniers. Celle-ci permet de rationaliser cette notion et de mieux l'appréhender dans le domaine militaire.

Application(s) : une typologie des usages militaires de l'IA

Comme de nombreuses technologies numériques aujourd'hui, l'IA trouve une part de ses origines dans le milieu militaire. Sciences techniques et art militaire ont toujours entretenu des liens forts tant l'avantage technologique pouvait procurer des

gains stratégiques, opérationnels et tactiques aux armées. Ainsi, l'*Office of Naval Research* du Département de la Défense américain (DoD), a par exemple participé au financement de la Conférence de Dartmouth en 1956. Ce sont alors les priorités militaires en matière de commandement et de contrôle, d'automatisation ou de surveillance qui vont orienter les recherches et les développements de l'IA dans le domaine des véhicules, de la commande par la parole ou de la vision par ordinateur. À partir des années 60, des chercheurs en IA ont bénéficié d'un soutien financier majeur de la *Defense Advanced Research Projects Agency*, agence de recherche et de développement en nouvelles technologies du DoD.

Le développement de l'IA ne s'est cependant pas fait de façon linéaire et le domaine a connu de nombreuses crises qui ont suivi le même schéma : les découvertes en IA, toujours teintées par l'ombre de la dimension mythique de l'IA, ont souvent provoqué des engouements et conduit à des promesses techniques qui dans les faits ne pouvaient être tenues. Les déceptions occasionnées, notamment des forces armées, ont instauré une méfiance envers les chercheurs en IA et plus largement le domaine, et donc une baisse, voire un arrêt, des financements en la matière. Ces phases décroissantes du développement de l'IA ont été qualifiées d'« hiver de l'IA ». La recherche en IA ne s'est cependant jamais totalement arrêtée et des avancées dans des domaines connexes ont souvent permis de nouvelles découvertes et un regain d'intérêt pour la matière.

Depuis les années 2010, les progrès des systèmes connexionnistes (apprentissage automatique) ont redoré le blason de l'IA et nourri un nouvel engouement qui n'échappe pas à un retour du discours mythifiant de l'IA. Entre les années 1960 et aujourd'hui, la capacité d'impulsion militaire en matière d'innovation technologique s'est cependant drastiquement réduite, notamment en IA. Cela s'explique, d'une part, par la méfiance des armées qui ont un budget limité pour investir dans des solutions technologiques comme l'IA qui a pu décevoir par le passé, et, surtout, par l'accaparement du développement des moyens numériques par quelques entreprises américaines. Les entreprises, aux côtés des universités, ont naturellement toujours été présentes dans le développement des disciplines contribuant à l'IA et ont toujours entretenu des contacts avec la sphère militaire. Par exemple, des représentants de l'industrie (IBM, Bell) ont participé à la Conférence de Dartmouth. Un processus d'oligopolisation du numérique constaté à partir des années 1990 a cependant fait de quelques entreprises américaines les leaders dans ce domaine. Face aux États-Unis, la Chine a rapidement rattrapé son retard et s'est inspirée de la politique libérale américaine de la Guerre froide pour développer ses propres géants du numérique prolifiques en IA. Les progrès de l'IA dans le domaine militaire dépendent donc pour beaucoup du rapport entre l'État et sa force industrielle, que ces rapports soient négociés ou imposés.

On peut distinguer trois catégories d'usages militaires de l'IA :

- Les SIA de *préparation à l'action*: ces systèmes soutiennent l'analyse et l'amélioration des facteurs nécessaires à la conduite des opérations, c'est-à-dire l'état des forces, l'état des systèmes et l'état de la situation. Dans chacun de ces domaines, les SIA apportent des améliorations substantielles. D'abord, et peut-être surtout, la situation militaire peut faire l'objet d'analyses par des SIA dans le domaine du renseignement, de la surveillance et de la reconnaissance (ISR). L'analyse de grandes quantités de données de nature et de sources très variées permet la détection de signaux faibles imperceptibles pour l'humain et à l'anticipation des menaces. Concernant l'état des forces, les SIA peuvent améliorer les conditions de formations et d'entraînements via des simulations ou du « Wargaming », mais aussi permettre une veille sanitaire avancée grâce à l'analyse des données de santé. Sur un versant plus logistique, les SIA peuvent assurer une veille des systèmes techniques grâce à une maintenance assistée ou « prédictive ».
- Les SIA de *soutien à l'action*: sur la base des analyses mentionnées, les commandants militaires prennent des décisions qui peuvent également bénéficier de l'assistance de SIA. Sur un plan formel, les SIA peuvent améliorer la communication, la synthèse et la présentation des informations récoltées sur l'état d'une situation militaire donnée afin d'améliorer sa connaissance par la force. Les armées qui développent des SIA visent aujourd'hui l'amélioration de connaissance situationnelle (*situational awareness*) et un combat dit collaboratif, c'est-à-dire une circulation rapide et précise de l'information en temps réel, entre toutes les entités afin d'améliorer la coordination des actions. Sur un plan plus matériel, les SIA peuvent formuler des recommandations à l'égard de certaines situations afin de proposer la solution la plus optimisée.
- Les SIA de *mise en œuvre de l'action*: les SIA peuvent également être pleinement utilisés dans la mise en œuvre des décisions militaires. Il convient ici de poser deux distinctions. D'une part, la distinction entre moyens cinétiques et non cinétiques. La nature numérique des SIA fait qu'ils peuvent être mobilisés dans les champs non cinétiques. Il y est ainsi possible d'employer des SIA dans le cadre de cyberopérations militaires ou d'opérations de désinformation en ligne. Plus classiquement, les SIA peuvent aussi être utilisés au sein de moyens cinétiques conventionnels comme des drones ou des systèmes de défense aérienne. D'autre part, la démarche de la mise en œuvre distingue le but de l'action (l'objectif mis en œuvre) et la façon dont elle l'est (le moyen de la mise en œuvre). Les SIA peuvent concourir à ces deux étapes. Dans le domaine cinétique, les SIA intégrés dans un drone peuvent contribuer aux tâches de navigation (moyen de la mise en œuvre), mais aussi au processus de ciblage (objet de la mise en œuvre). De même, dans le domaine de la désinformation, un SIA peut être employé pour créer un contenu de désinformation personnalisé et crédible (par exemple un *deepfake* – l'objet de la

mise en œuvre) et des SIA pourront le diffuser rapidement et à grande échelle sur divers réseaux (moyen de la mise en œuvre).

En raison du caractère générique de l'IA, ces catégories sont poreuses et l'on observe un *continuum* entre les trois types de systèmes. Les SIA de *préparation à l'action* qui récoltent et traitent des renseignements militaires serviront aux SIA de *soutien à l'action* qui permettront la formulation de recommandations. Ces dernières pourront ensuite être directement opérationnalisées par un SIA de *mise en œuvre* de l'action militaire. La réunion de ces SIA dans une optique de combat collaboratif permettrait selon certains États une amélioration et une accélération de la prise de décision constituant un avantage militaire décisif. Cela a conduit ces États à considérer cet objet comme une technologie de rupture qui changerait de façon structurelle les capacités militaires et ainsi la face de la guerre.

Les ambitions prêtées aux conséquences de l'IA dans la guerre ont pris la forme de stratégies étatiques, sortes de prophéties autoréalisatrices qui s'évertuent à décrire la façon dont les SIA sont et seront intégrés dans la sphère militaire et changeront la manière de faire la guerre. Ainsi, le DoD a élaboré, depuis 2019, pas moins de [sept stratégies](#) relatives à l'IAM. La [France](#), le [Royaume-Uni](#), [l'OTAN](#) et [l'Inde](#) ont également publié des documents dédiés aux enjeux et objectifs relatifs à l'intégration de l'IAM dans leurs institutions militaires. Sans avoir un document stratégique militaire spécifique sur l'IAM, d'autres États comme la [Chine](#) ou la [Russie](#) évoquent largement cette technologie au sein de documents de perspectives militaires plus transversaux ou de stratégie nationale relative à l'ensemble des usages de l'IA. Bien qu'elles n'exposent pas les réelles capacités techniques de ces États, il ressort de cette surabondance de stratégies une impression de « course à l'IAM », ou du moins de course à la conceptualisation militaire de cette technologie. S'il est indispensable pour ces États d'indiquer leurs efforts dans ce domaine, il demeure un risque toujours plus grand d'une déconnexion entre d'un côté la communication technologique militaire et de l'autre, la réalité technique et opérationnelle des SIA militaires. Seul l'usage des SIA sur le terrain militaire pourra attester de la crédibilité de cette dynamique.

Intégration : le cas de la guerre en Ukraine

La guerre en Ukraine offre malheureusement une situation particulièrement propice à l'examen des usages de l'IAM au sein d'un théâtre d'opérations. Cette [guerre majeure](#) qui oppose deux États avec des capacités militaires avancées, propres ou issus d'une aide extérieure, permet d'analyser la façon dont l'IA est intégrée dans leurs capacités et si cela correspond aux discours professés à son égard.

S'il est fort probable que des SIA militaires sont utilisés dans cette guerre, il s'avère difficile de le certifier. D'une part, les principales informations relatives à l'utilisation de SIA proviennent souvent d'acteurs qui ont un intérêt à les valoriser, que cela soit les États engagés dans le conflit ou qui soutiennent l'un d'eux, les entreprises qui produisent et vendent ces technologies ou la société civile qui les dénonce. D'autre part, peu importe la bonne foi ou l'intérêt de l'acteur à arborer l'utilisation de l'IA, rares sont ceux qui, compte tenu de l'absence de consensus dans ce domaine, prennent la peine de préciser leur conception. Ce flou permet ainsi aux différents acteurs de faire des déclarations qu'on ne peut pas toujours vérifier dans les faits.

Le cas des drones utilisés par les deux parties illustre ces difficultés. Il a par exemple été allégué l'utilisation de drones kamikazes par l'Ukraine ([Switchblade](#)) et la Russie ([Lancet](#), [Koub-BLA](#)). Ici, l'IA est très souvent associée à l'autonomie de ces systèmes, que ce soit l'utilisation de SIA pour la navigation (décollage, vol, atterrissage), la récolte d'informations ou même la mise en œuvre du ciblage. On le sait, l'acception du terme « autonomie » peut être plurielle. Par exemple, pour [certains](#), l'autonomie visera le simple fait que la munition attendra seule une cible déterminée par l'homme, tandis que pour d'autres cela comprend également la détermination de la cible selon des critères définis humainement de façon plus ou moins précise. En outre, il est complexe de savoir si le drone est entièrement piloté à distance ou si sa navigation est facilitée par des SIA qui permettent l'autonomisation de certaines tâches. Les spécificités variables de chaque système accentuent d'autant plus ce flou. Nombre d'experts cependant [considèrent](#) qu'une majorité des drones mentionnés dans cette guerre sont contrôlés par l'humain et que les fonctions autonomes n'interviennent qu'à la marge.

Une faible autonomie dans ces drones ne signifie pas qu'il n'y a pas de SIA. D'une part, parce que des SIA sont probablement utilisés pour l'autonomisation de ces fonctions, d'autre part parce que des SIA peuvent être présents pour récolter et trier les données, ou informer le processus de ciblage, sans que cela soit matérialisé par une action autonome du système. La présence de SIA de reconnaissance faciale dans des drones a par exemple souvent été [attestée](#). Ainsi, même en adoptant une définition restrictive de l'IA, il est fort probable que celle-ci soit observée dans les drones utilisés lors de cette guerre, mais pas de façon décisive et encore moins de la manière dont cela est annoncé dans les stratégies des États. En outre, l'utilisation de SIA au sein de [cyberopérations](#) et [d'opérations](#) de [désinformation](#) ont été rapportées tant du côté [russe qu'ukrainien](#). Des SIA auraient aussi

été utilisés pour détecter et contrer ces opérations en attestant l'utilisation de *deepfake* ou en élaborant des mesures de cybersécurité. La vulnérabilité des SIA aux cyberopérations a par ailleurs souvent été soulignée. Il s'agit donc d'une dimension à prendre en compte, bien que cela n'ait pas été encore signalé.

En dehors de ceux présents dans les drones, des SIA de préparation et soutien à l'action ont également été employés pour traiter l'information et orienter la décision militaire. C'est notamment le cas en Ukraine grâce à l'aide d'entreprises américaines comme Clearview qui a fourni ses SIA de reconnaissances faciales pour détecter les soldats russes et identifier les morts et les blessés ; Space Know qui a mis à disposition des SIA d'analyses d'images satellitaires pour détecter l'activité des forces russes en continu et les mouvements de population ; Snorkel AI qui a permis l'analyse des signaux et les communications de la Russie, identifier les informations de grande valeur et les utiliser pour guider la prise de décision et Primer afin d'intercepter, analyser, transcrire et traduire les communications militaires russes. Le directeur de Palantir a également attribué la remarquable résistance de l'Ukraine à l'utilisation de SIA par ses forces armées, ceux de Palantir en l'occurrence.

On peut ainsi tirer quelques enseignements de ces utilisations. Les SIA sont avant tout utilisés dans le domaine immatériel soit à des fins d'ISR et d'aide à la décision, soit pour mener des opérations dans le domaine cyber et de la désinformation numérique. Dans ces deux cas d'utilisation, les SIA n'ont pas un effet aussi décisif que l'on aurait pu attendre à la lecture des stratégies étatiques. Pour le premier, la qualité des informations obtenues par SIA et leur apport pour les opérations ne sont pas explicites. Pour le second, si les usages sont incontestables, c'est l'échelle de leur utilisation et les conséquences sur le conflit qui peuvent apparaître décevantes. Plus largement, la communauté des experts travaillant sur l'IAM s'attendait à un emploi beaucoup plus massif eu égard aux annonces dans ce domaine. On perçoit que dans les faits l'utilisation de SIA reste assez modeste. Plusieurs facteurs peuvent venir expliquer cela dont certains peuvent s'avérer instructifs pour l'intégration de l'IA par les autres armées.

Une première série de facteurs concernent la situation spécifique de la Russie. Le régime rencontrerait déjà de nombreuses difficultés techniques qui dépassent le cadre de l'IA. La Russie ne se serait pas attendue à une résistance ukrainienne aussi efficace et n'aurait dès lors pas adapté ses moyens militaires, du moins dans un premier temps. Par ailleurs, les sanctions étrangères, qui affectent l'importation de biens, et la fuite d'une partie de la main-d'œuvre qualifiée auraient drastiquement entravé les capacités de développement russes en IA, notamment dans le domaine militaire. D'autres facteurs sont plus généralement relatifs aux conditions d'intégration des SIA dans les armées. Il pourrait d'abord s'agir de risques relatifs à un manque de formation du personnel, ou de techniciens spécialisés, pour l'utilisation de SIA qui nuirait à un usage serein de la technologie. En outre, il a été avancé que la nature chaotique du terrain militaire était difficilement appréhendable par les SIA. Par ailleurs, les forces armées russes auraient émis des doutes sur la fiabilité de leurs SIA, notamment au sein des drones, en raison de tests limités ou inexistants. Plus généralement, il manquerait une uniformité dans les méthodes destinées à tester les SIA et la certification de ces systèmes se serait avérée complexe. Les SIA seraient de surcroît particulièrement vulnérables à des cyberopérations qui visent leurs données d'apprentissage et altèrent donc leurs résultats. En conséquence, il y aurait eu une volonté de ne pas leur déléguer des fonctions trop importantes qui mettraient en jeu des objectifs militaires ou des vies humaines.

En dépit des stratégies militaires qui annonçaient une rupture dans la guerre causée par les SIA, le terrain ukrainien prouve que si des avantages sont perceptibles, ils sont encore loin d'avoir atteint les ambitions énoncées. Si les SIA militaires n'ont pas bouleversé la guerre en Ukraine, cette guerre a certainement enrichi le savoir et les pratiques relatives à l'utilisation de cette technologie. Les SIA, qui fonctionnent sur la base de l'apprentissage à partir de données, ont pu récolter de nombreuses informations militaires, notamment sur les actions et capacités des États belligérants, qui serviront à entraîner des SIA utiles dans des conflits contre ces États ou d'autres. En outre, ce conflit a permis d'expérimenter des SIA et de développer des pratiques qui méritent toutefois d'être minutieusement analysées en raison du risque de la cristallisation d'utilisations litigieuses de cette technologie.

Conclusion

En somme, la guerre en Ukraine ne sera pas la guerre de l'IA, mais elle contribue certainement à ses prémices. Lorsque la guerre du Golfe a été qualifiée de première guerre de l'espace, des ressources spatiales avaient déjà été utilisées dans des conflits antérieurs, mais n'avaient pas eu un rôle et une efficacité aussi importants que lors de cette guerre. On peut donc présumer que l'utilisation de SIA militaires suit cette trajectoire, cela d'autant plus que certains SIA fonctionnent généralement sur la base de l'apprentissage, ce qui n'aura de cesse d'améliorer leurs performances au long des conflits où ils seront mobilisés. Il restera à voir comment cette technologie serait utilisée dans un conflit par d'autres États, par exemple les États-Unis et la Chine.

Louis Perez, « L'intelligence artificielle militaire : du rêve au glaive », *Le Rubicon*, vol. 3, 25 mai 2023 [<https://lerubicon.org/lintelligence-artificielle-militaire-du-reve-au-glaive/>].