Le Président et le Comité de rédaction vous souhaitent ainsi qu'à vos proches une excellente année 2026, avec tous leurs vœux de bonne santé et de réussite dans vos activités tant professionnelles que privées.

Le mot du Président

Chers membres et amis de l'association AED/SNC-IHEDN,

C'est avec un grand plaisir que je vous présente le dixième numéro du bulletin Athéna. Nous avons réalisé 5 numéros au 2025. Nous continuerons cette année grâce à vos précieuses contributions. Ce numéro marque une nouvelle étape dans notre démarche collective de réflexion et de diffusion des enjeux stratégiques contemporains, élargie aux sessions SNC depuis notre rapprochement à l'été 2025.

En cette nouvelle année 2026, nous vous souhaitons, ainsi qu'à vos proches, une excellente année, tous leurs vœux de bonne santé et de réussite dans vos activités tant professionnelles que privées. Que cette année soit pour vous synonyme de prospérité et d'épanouissement !

Pour ce numéro 10, nous avons le plaisir de vous proposer plusieurs articles autour de l'intelligence artificielle. Notre conférence mensuelle Athena de décembre était d'ailleurs sur l'entraînement des modèles d'IA. Vous étiez une centaine à y participer à l'école militaire.

Vous pouvez dès à présent noter dans vos agendas le PDSF (*Paris Defence and Strategic Forum*) organisé par l'ACADEM, dont nous sommes partenaire, du 24 au 26 mars, et nos XIX^{e} EAS (Entretiens Armement et souveraineté) le 8 avril après-midi. Venez nombreux vous enrichir et partager nos réflexions.

En vous remerciant de votre fidélité et de votre engagement, je vous invite dès à présent à renouveler votre cotisation pour 2026. Nous avons besoin de votre soutien. Le lien est en ligne sur notre site Internet : www.aed-Ihedn.fr .

Très amicalement,

Géraud BRUN, Président de l'association AED/SNC-IHEDN

Sommaire

Ce numéro regroupe plusieurs articles sur l'intelligence artificielle et ses impacts actuels et potentiels sur les armements et plus généralement sur les conflits militaires. Un quatrième texte proche du même sujet concerne la guerre informationnelle.

Le mot de la rédaction

Chers membres d'AED/SNC-IHEDN,

Le Bulletin d'Athéna nouvelle formule, donnant la parole aux membres de notre association des auditeurs des sessions AED, maintenant élargie aux sessions SNC, a atteint son régime de croisière.

La rédaction remercie particulièrement les auteurs des 31 articles qui ont alimenté les 5 numéros de l'année 2025.

La rédaction ne doute pas que l'année 2026 sera aussi fructueuse, mais elle le sera grâce à vous, lecteurs-auteurs ! N'hésitez pas à proposer des articles, concernant, notamment :

- des évènements d'actualité, mais impactant l'avenir (comme la *National Security Strategy* de la présidence américaine) ;
- l'avancement de recherches ou de programmes d'armement et l'impact présent ou potentiel des innovations de toute nature sur les armements et leur utilisation ;
- vos réactions à des articles parus antérieurement ; notre Bulletin est ouvert à des forums de débat.

Vos contributions sont à adresser à bulletin.athena@aed-ihedn.fr

Parmi vos priorités pour 2026, mettez en bonne place :

Écrire un article pour le bulletin Athéna !

Rendez-vous d'Athéna

L'association 3AED-IHEDN propose un rendez-vous mensuel autour de conférences qui permettent d'approfondir des questions en lien avec les thématiques d'économie de défense, d'armement, d'innovation et de géopolitique, avec des spécialistes reconnus dans leur domaine.

Nommé "Les Rendez-vous d'Athéna" en référence à la déesse de la stratégie militaire et de la sagesse chère à la communauté IHEDN, ce cycle est proposé aux membres de l'association et des associations partenaires à jour de leur cotisation. Ces conférences sont organisées conjointement avec l'association de l'Armement terrestre (AAT) et avec le soutien de la société ALCIMED.

Ces conférences ont lieu au rythme d'une par mois. Leur organisation présente souvent quelques aléas (orateurs se décommandant car non-disponibles à la date prévue, cas le plus courant). Aller sur notre site Web pour être au courant des modifications éventuelles de dernière minute.

Ces conférences sont généralement enregistrées et consultables en replay sur notre site internet www.aed-ihedn.fr les tableaux qui suivent donnent la liste des conférences de 2025 disponibles et une liste des premières conférences programmées pour 2026.

PROGRAMME DES CONFÉRENCES POUR 2025		
Date	Thème	Commentaires
Mardi 21 janvier	Athéna #1 : L'évolution de la bataille balistique, enjeu des futurs conflits	Orateurs: Younik Thomas et Thomas Merlin (Arianegroup)
19 février	Athéna #2 : L'industrie en temps de guerre : RETEX Ukraine avec vision étatique et vision terrain	Orateurs: Géraud Brun & Xavier Tytelman
13 mars	Athéna # 3 : Éthique de l'IA	Orateur : Alexei Grinbaum (CEA)
15 avril	Athéna # 4 : Basculement climatique et conséquences pour les forces armées	IRIS Responsable du Programme Climat, Energie et Sécurité Orateurs : Julia Tasse et Mathilde Jourde (IRIS)
24 Juin	Athéna # 6 : Economie de guerre et anticipation stratégique.	Table ronde : animée par Grégory Chigolet (Conseiller économique de l'état-major des Armées) + IGA Walter Arnaud (DGA) + Dr Sylvain Moura (France Stratégie)
8 juillet	Athéna # 7 : La réserve opérationnelle industrielle Orateur : ICA Patrick GRELIER	
24 septembre	Athéna # 8 : La stratégie d'influence de la France au Magreb	Oratrice : Imen Chaanbi (consultante géopolitique zone Afrique MO)
21 octobre	Athéna # 9 : BITD Maroc Algérie	Orateur : Patrick Michon

20 novembre	Athéna # 10 : AALTO : Le futur de l'aviation stratosphérique	Orateur : Hugues Boulnois : CEO de AALTO : filiale de AIRBUS qui développe un HAPS, le Zéphir
16 décembre	Athéna # 11 : L'entrainement des Intelligences Artificielles	Couplé avec la CHAIRE CYBER Table ronde : animée par Vincent Giraud

Conférences 2026

13 janvier	Athéna # 1 : La navigation magnéto-inertielle	David Vissière Président de SYSNAV, le lauréat du dernier prix « AAT - Ingénieur Général Chanson
17 février	Athéna # 2 : Le financement européen de la défense	Nicolas Jean Brehon (Conseiller honoraire au Sénat, spécialiste des questions budgétaires)
12 mars	Athéna # 3 : anxiété géopolitique : Enjeux et défis pour la décision et l'action	Mathieu Guidère (Professeur des Universités et Directeur de recherches à l'INSERM)

Défense et intelligence artificielle

Jacques Bongrand SN (CHEAr) 25

Depuis quelques années, les applications de plus en plus nombreuses de l'intelligence artificielle font l'objet de multiples alertes médiatiques. Elles méritent d'autant plus d'être examinées dans le domaine de la défense qu'il est essentiel pour un État de ne pas se laisser surprendre ou dépasser par des ennemis cachés ou potentiels. C'est pourquoi il est intéressant pour les lecteurs du Bulletin Athéna de s'informer des différentes études accessibles à ce sujet.

Parmi ces études, figure un rapport issu d'une coopération avec le Conseil général de l'armement et publié en décembre 2025 sur le site de la Société des ingénieurs et scientifiques de France, (www.iesf.fr, publications, cahiers thématiques). Quelques aspects significatifs en sont présentés ci-dessous.

Une vision d'ingénieurs généralistes

Concernant l'intelligence artificielle, comme plus généralement en matière de renseignement militaire, la plus grande partie des informations utiles est publique. L'enjeu est d'en faire une exploitation dont la difficulté tient d'une part à l'extrême imbrication des acteurs, des applications possibles et des secteurs impactés, d'autre part à l'évolution particulièrement rapide de l'état de l'art.

Dans ce contexte les membres du groupe de travail, ingénieurs généralistes plutôt que chercheurs spécialisés, ont voulu rassembler le plus clairement possible et dans un volume raisonnable (une cinquantaine de pages) un ensemble de données pertinentes afin d'en tirer une vue d'ensemble, au niveau de notre société, puis plus particulièrement de la défense, et des recommandations pratiques à court terme.

Une transformation profonde et encore peu prévisible de nos sociétés

Entre autres, trois points sont à souligner.

Avant tout, il paraît inévitable que les évolutions techniques en cours provoquent une modification des comportements individuels courants qui constituera à terme un facteur de transformation de nos sociétés, susceptible d'influencer significativement leur capacité de réaction à certaines attaques. Paradoxalement, on pourrait constater à la fois une diminution de sens critique élémentaire liée au recours systématique à des données mises en forme ou à des assistants informatiques et une conscience croissante des possibilités de manipulation.

En outre, les ingénieurs devront adapter leur action d'abord pour utiliser efficacement les modèles en posant les questions appropriées, ensuite pour apporter une garantie de confiance aux résultats obtenus, et aussi pour rechercher des visions de synthèse et des solutions innovantes plus originales que celles fournies par les intelligences artificielles.

Enfin, dans la compétition en cours entre différents acteurs mondiaux, face au risque de dépendance envers des géants américains ou chinois qui ont consenti des investissements colossaux, la recherche d'une souveraineté numérique est de plus en plus cruciale au niveau de la France ou de l'Europe, alors même que cette dernière apparaît en retard pour les réalisations et en avance pour la réglementation de l'intelligence artificielle.

Des conséquences importantes dans le domaine de la défense

Il importe à l'évidence de se préparer à affronter des menaces sans précédent tout en tirant le meilleur parti de capacités accrues.

L'amplification des menaces est à attendre notamment de deux causes : l'intelligence artificielle permet d'utiliser comme armes des machines largement répandues dans le domaine civil, dont les drones sont l'exemple le plus connu, et de s'attaquer à des cibles de plus en plus variées et précisément visées. En raison des possibilités nouvelles et relativement accessibles qu'elle offre, des dommages importants sont susceptibles d'être provoqués par des agresseurs plus divers que par le passé, tels que des organisations non gouvernementales, terroristes ou maffieuses, éventuellement manipulées par des États..

Par ailleurs les armements traditionnels, qu'il s'agisse par exemple de véhicules de combat, de canons ou de missiles, seront de plus en plus autonomes et connectés entre eux, donc plus efficaces, mais aussi d'un comportement moins prévisible et plus difficile à maîtriser par les opérateurs.

À côté des armements eux-mêmes, la fonction de commandement disposera de moyens considérablement renforcés, d'abord pour planifier des opérations plus difficiles à prévoir en s'appuyant sur des données beaucoup plus nombreuses et variées, ensuite pour évaluer des situations en temps réel afin de prendre aussitôt les décisions les plus appropriées.

Toutes ces évolutions ne seront pas sans conséquences sur les aspects éthiques, alors que les combattants deviendront davantage des opérateurs éloignés du champ de bataille et moins directement reliés aux victimes des affrontements. La question suivante peut ainsi être posée : des erreurs inexpliquées de l'intelligence artificielle sont-elles tolérables si elles sont moins graves ou fréquentes que les erreurs humaines inévitables ?

Des mesures évolutives à prendre sans tarder

Face à ces perspectives, il importe d'entreprendre sans tarder des adaptations, même s'il semble certain que ces dispositions devront être périodiquement revues au fur et à mesure que le phénomène de l'intelligence artificielle sera mieux cerné. Entre autres, quatre observations sont esquissées ci-dessous.

Une première orientation évidente consiste à développer et entretenir une connaissance de cette technologie dans l'ensemble de la population, par des modules d'initiation et de mises à jour périodique. Mais, parallèlement, il conviendra de maintenir une capacité à prendre du recul par rapport à ces outils et à s'en passer éventuellement, en particulier en matière de défense pour traiter dans l'urgence des situations imprévues ou pour opérer dans des conditions dégradées.

En second lieu, pour progresser sans tarder vers une meilleure souveraineté numérique, une loi de cadrage et de programmation pourrait définir les fournisseurs, les approvisionnements essentiels et les compétences à maîtriser, associés à des périmètres de sécurité visés (national, européen ou mondial), en cohérence avec les moyens financiers consentis.

Une troisième constatation est qu'un effort particulier de clarification du rôle des acteurs publics concernés s'impose du fait de l'extrême diversité des usages de l'intelligence artificielle. Cette remarque concerne notamment au ministère des Armées la Direction générale du numérique, la Direction interarmées des réseaux d'infrastructure et des systèmes d'information, l'Agence du numérique de défense et l'Agence ministérielle pour l'intelligence artificielle de défense. Il convient par ailleurs de citer l'Agence nationale de la sécurité des systèmes d'information.

Enfin, un objectif à poursuivre est de mieux concilier la préoccupation d'efficacité conduisant à élargir autant que possible les bases d'entraînement et les cercles d'utilisateurs de tout

modèle d'intelligence artificielle, avec le souci de sécurité qui induit une limitation des accès directs ou indirects à ces bases d'entraînement. Il serait sans doute utile, au ministère des Armées, d'établir une liste de modèles spécialisés pour chacun desquels une autorité serait désignée et chargée de tenir à jour le réseau des utilisateurs.

Une question adressée à chaque lecteur

Osons conclure cet article, et plus précisément ces recommandations, par une remarque à caractère philosophique : face à un problème complexe, une tendance logique et naturelle est de rechercher les acteurs les mieux placés pour mettre en œuvre une solution et d'énoncer ce qu'ils devraient faire selon nous. Le rapport qui vient d'être présenté n'échappe pas à cette règle. Mais ne serait-il pas plus constructif que chaque lecteur se demande quelle contribution, même modeste, il peut lui-même apporter ?

Il s'agirait d'ailleurs d'une application de la question adressée à chacun qui conclut mon livre intitulé « Reconnaître notre destinée », que le bulletin d'Athéna m'a permis d'évoquer dans son numéro 5 :

Que faire ici et maintenant pour améliorer ce monde ?

Bonne réflexion à tous…

L'intelligence artificielle de défense

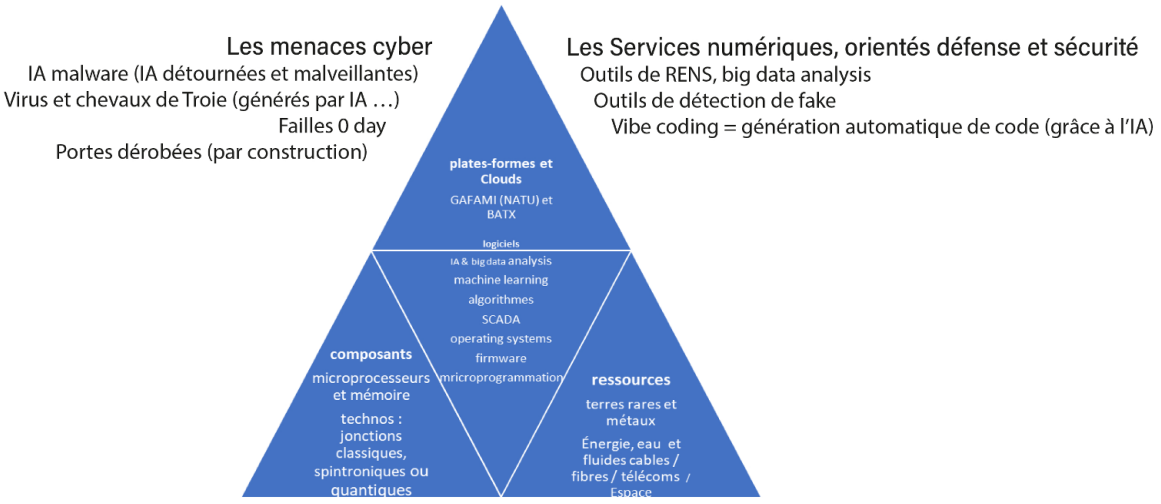
Sylvain Delaitre

Rappel de la structure des systèmes numériques

Le numérique quel qu'il soit

La topographie du numérique s'étend sur deux niveaux principaux entrelacés, une sous structure matérielle et une surstructure logicielle, elle-même constituée de plusieurs couches (des couches de base, comme le logiciel système qui fait tourner la machine aux couches applicatives finales, en passant par des couches intermédiaires de progiciels qui facilitent la réalisation de ces applicatifs).

La pyramide du numérique représentée ici donne une idée générale de l'ensemble industriel, remontant pour le matériel aux intrants nécessaires, car la logistique de ces intrants, qui a peu à voir avec le numérique, tel qu'on l'entend habituellement, n'en est pas moins une source de vulnérabilités à ne pas oublier.



Après ce rappel très schématique du numérique général, abordons l'IA, et, d'abord, par un court historique.

L'intelligence artificielle

Historique de l'IA

Ce qu'on appelle IA (informatique avancée ? Informatique approximative ? Informatique apprenante… ?) est la fille de la cybernétique, des asservissements et de la programmation (machine universelle de Turing, architecture de Von Neumann).

- Un des parents est le traitement du signal, développé à partir de 1930, dans les cadres des transmissions, du radar et du sonar (asdic à l'époque).
- Autre parent, la théorie et la pratique des asservissements : dès le début du XXe siècle, stabilisation des tourelles d'artillerie navale, 1938 : premiers asservissements (suivi de cible) dans le domaine de la défense antiaérienne.
- Une ascendance capitale : les calculateurs. Sans remonter à Pascal et à Babbage :
  - premier réseau de calcul en 1940 (avec des relais téléphoniques),
  - premier neurone formel (McCulloch & Pitts, 1943) — avant les ordinateurs !
  - premiers vrais ordinateurs programmables en 1945 (États-Unis et Angleterre à Manchester — États-Unis pour le projet Manhattan, en Angleterre pour la cryptologie avec Turing, notamment)

L'idée que la machine puisse un jour égaler, voire surpasser l'homme apparaît dès le premier ordinateur programmable opérationnel (article de Turing dans Mind), les choses s'enchaînent ensuite :

- conférence de Dartmouth en 1956, création de l'acronyme IA (*Artificial Intelligence*) ;
- premier neurone artificiel, le *Perceptron* (Rosenblatt, 1958), modèle linéaire à seuil, connexions modifiables ;
- Perceptrons multicouches : Rétropropagation du gradient (Parker 1982, Le Cun 1985, Rumelhart & McClelland 1986).

Après un creux à la fin du siècle, la première famille d'intelligence artificielle, la famille symbolique, celle des systèmes experts (approche formelle, corpus de règles), alors au premier plan de la recherche académique, s'étant révélée décevante, la recherche reprend fortement après 2000, surtout autour d'une nouvelle piste, la deuxième famille d'intelligence artificielle, que l'on peut appeler famille connexionniste, qui abandonne l'approche des sciences physiques classiques (mesurer, théoriser) pour une approche purement heuristique et probabiliste via l'apprentissage de réseaux de neurones cherchant à imiter le fonctionnement du cerveau humain ; à côté de la recherche académique, elle suscite rapidement, dès les premiers espoirs de succès, un très important volet de recherche-développement industriel, notamment aux États-Unis. Cette voie représente 99 % des applications actuelles.

Essai d'explication simple de l'apprentissage et du fonctionnement des réseaux de neurones

Ces réseaux calculent une fonction d'un paramètre d'efficacité appelé coût (sommairement l'écart entre le résultat obtenu et la réalité), qu'ils optimisent (recherche d'un optimum relatif) via la rétropropagation de l'erreur (lors de la phase d'apprentissage) et la méthode de descente de gradient. D'abord très simples (matrices de 16 x 16, 3 ou 4 couches dédiées aux traitements d'images), ces réseaux se sont approfondis et complexifiés (connexions réentrantes) et, surtout, fortement élargis.

Les réseaux de neurones (que l'on pourrait assimiler à un bricolage plus ou moins à l'aveugle) ont (provisoirement ?) gagné aujourd'hui sur les systèmes experts parce que la puissance brute de calcul (avec l'arrivée des GPU à partir de 2006) permet de faire tourner d'énormes réseaux de neurones artificiels (gigantesques matrices de corrélation) pour des réponses en un temps « raisonnable ».

Cette puissance a permis à Yann Le Cun de gagner en 2012 le concours international de reconnaissance d'image ImageNet grâce à ses réseaux de neurones, la course est dès lors lancée.

Cette évolution énorme de la puissance de calcul accessible : le Cray-1 en 1980, la merveille, faisait 160 millions de flops (1,6 108 d'opérations par seconde) ; on en est aujourd'hui à l'exaflops (1018). Cette puissance de calcul permet de développer de nouveaux réseaux de neurones, les LLM *Large Language Models*, les grands modèles de langage, basés sur les probabilités conditionnelles, pour créer des phrases, puis des textes complets, via d'énormes bases d'apprentissages (40 000 mots par langue, et une partie d'Internet…).

Une des idées qui a été déterminante dans l'explosion actuelle est la « tokenisation » des mots, on entend par là le fait de faire travailler les réseaux de neurones non sur les mots d'une langue, un corpus énorme, mais sur les éléments linguistiques constitutifs des mots ou notions qu'ils portent (pas exactement les syllabes, mais dans la même idée). Les tokens d'une langue (voire d'un groupe de langues) forment un ensemble beaucoup plus petit que celui des mots. Autres concepts déterminants, la vectorisation et l'architecture GPT *(Generative Pre-trained Transfer)*, ces deux approches, prises isolément ou conjuguées, permettent une réduction importante de la charge de calcul et donnent une efficacité en temps quasi réel à ces outils. Ces outils numériques (opérant sur de gigantesques matrices de nombres), travaillent dans des espaces virtuels avec de très nombreuses dimensions (des milliards !), les résultats obtenus correspondant aux projections des mots ou autres entités linguistiques sur les vecteurs propres du (très grand) système. Des vidéos pédagogiques sérieuses expliquent le principe des LLM et des GPT sur Youtube (Cours sur les LLM type GPT - YouTube)

Ceci a permis le lancement de *ChatCGPT* en version grand public en novembre 2022. Depuis, de nombreuses applications se font concurrence et l'évolution est extrêmement rapide (il y a une bonne dizaine d'offres sur le marché, avec de nouvelles versions qui s'enchaînent très rapidement).

Pour donner une idée de la puissance de calcul mobilisée, la tokenisation se faisait au début en prenant en compte un environnement de quelques mots, elle se fait aujourd'hui en utilisant le contexte de 200 pages de texte afin d'assurer la cohérence…

Tout cela a cependant un prix matériel élevé. Malgré la baisse continue et spectaculaire de la consommation par unité de calcul (consommation par flops, par exemple, de 30 joules par addition pour l'ENIAC aux GPU NVidia de 2022 : 1,5 10-12 joule par opération), les Data centers (pour les bases de l'apprentissage et la gestion des requêtes) et le numérique général représentent, malgré cette sobriété 3 % de la consommation mondiale d'électricité, les investissements annoncés annuels mondiaux pour les data centers devraient atteindre 600 milliards de dollars en 2026, dont beaucoup aux États-Unis dont le réseau électrique (qui n'est peut-être pas le plus performant) risque la surchauffe, ce qui pousse les grands opérateurs à commander des centrales nucléaires privées (SMR).

Peut-on tenter de prévoir l'avenir ? Ce n'est pas sûr, mais il est permis d'essayer !

Perspectives d'évolution

Les recherches et développements les plus prometteurs portent sur :

- les IA hybrides (symbolique + neuronale), les IA ancrées dans la physique et dans le Réel (V-JEPA de Yann LeCun en décembre 2025) ;
- les agents intelligents, qui promettraient une forme d'autonomie de coordination et d'autonomisation des systèmes opérationnels ? (extension de la cybernétique vers les couches hautes de l'Informatique ou recyclage marketing ?)

– les IA frugales et localisées (pas de grandes bases d'apprentissage, pas d'énormes besoins en Cloud…)
– …

Après cette introduction condensée, on peut maintenant aborder le cœur du sujet de cet article, les outils IA dans la défense. Il est utile de les classer en deux catégories, les applications génériques, comme le sont en informatique classique les applications de bureau, et les applications spécifiques au domaine de la Défense.

Les militaires, le « madame ou monsieur Tout le monde » de l'IA

Parce qu'ils sont « comme tout le monde », les militaires adoptent les outils disponibles de l'IA grand public ; secteur qui pèse 550 millions d'utilisateurs hebdomadaires réguliers (statistique mondiale) en juin 2024, et 900 en décembre 2025.

Cette adoption massive, permise par la mise en ligne gratuite (ou pour un faible abonnement) d'outils interactifs en temps réel, pour le grand public, les entreprises et les administrations — grâce au développement de modèles toujours plus puissants et efficaces — a conduit à la diffusion mondiale et globale (quasiment tous les métiers, tous les domaines sont concernés) de l'IA. On est en présence d'un phénomène historique, du même ordre que la révolution Internet ou, antérieurement, de l'arrivée des ordinateurs personnels, avec le lancement du premier Mac en 1984.

Les outils IA actuellement disponibles permettent :

– des réalisations virtuelles entièrement nouvelles (IA génératives de textes, images, courtes vidéo…) ;
– la rédaction rapide de rapports et synthèses (LLM) (pas utilisé pour cet article…) ;
– la recherche documentaire (Perplexity…)

Finalement, cette acculturation de l'IA par les utilisateurs (volontaires ou poussés à le faire par leur entreprise) se fait assez naturellement, par diffusion des applications simples d'emploi et réellement utiles (ou perçues comme telles).

Cette utilisation massive des outils « publics » de l'IA par les personnels de la Défense pose des problèmes d'hygiène informatique (risques classiques cyber) et surtout d'étanchéité des systèmes d'information : comment ne pas laisser fuir des informations sensibles, ou simplement « intéressantes » via les outils de l'IA et les clouds externes… puisqu'une grande partie de ces applications ne sont pas locales (sur la station de travail de chacun), ni même sur les serveurs locaux ou centralisés de son organisation, mais sur les serveurs (clouds) des grands fournisseurs (GAFA et autres).

L'irruption de formes nouvelles d'automatisation des tâches quotidiennes impacte également l'organisation du travail en tant que telle, cela doit s'anticiper et se préparer…

De plus, plusieurs problèmes demeurent, face à cette irruption globale des outils IA :

– les doutes sur la pertinence et la fiabilité des réponses produites par les services publics d'IA (si on n'est pas spécialiste d'un domaine ; comment vérifier que l'outil « dit vrai », n'hallucine pas ou ne comporte pas de biais systématique ? — L'outil Grok d'Elon Musk, notamment, est, à tort ou à raison, accusé d'être polarisé…) ;
– la question des gains de productivité reste très controversée, trois ans après l'arrivée des GPT : des expertises reconnues laissent entendre que les promesses du marketing sont très au-dessus de la réalité de terrain… (cela fait partie de ce que certains appellent « la bulle de l'IA »), cela avait d'ailleurs aussi été le cas pour les précédentes révolutions informatiques.

Les utilisations spécifiques de l'IA en défense

On aborde là le cœur du sujet militaire.

La grande force des IA actuelles pour les applications défense réside essentiellement dans les capacités suivantes :

– optimisation des systèmes complexes (conception, utilisation) ;

- classification – discrimination (selon des métriques complexes) ;
- mise en évidence de corrélations cachées et détection d'évènements rares ;
- prédiction d'évènements ou d'états opérationnels.

Comment cela se décline-t-il dans les différents secteurs opérationnels ?

C4ISR = commandement, contrôle, surveillance, reconnaissance

Le concept de champ de bataille numérique et infocentré a été développé à partir de la fin des années 1990.

Les progrès récents des outils IA permettent, de façon générale, une accélération du cycle de renseignement et de décision, ainsi qu'une meilleure anticipation et une meilleure profondeur d'analyse (situation, logistique…).

Les outils IA s'insèrent nativement dans l'espace cyber et numérique, ils s'interfacent ainsi naturellement avec les outils opérationnels modernes. Restent les questions du choix des architectures et de la disponibilité des capacités de calculs indispensables à l'IA…

Boucle OODA

Les outils IA interviennent dans les quatre étapes définies par cet acronyme :

O = observer

Aide et optimisation de la détection

Le *Big data analysis* aide à la détection d'évènements rares et de menaces « sous les radars ». L'IA peut produire des prédictions sur la base des probabilités conditionnelles (estimées, pas toujours très précisément…)

O = orienter

Classification des menaces. En langage technique, les algorithmes d'IA peuvent calculer des distances dans des espaces multidimensionnels complexes, traduit en langage naturel, ils peuvent établir dangerosités relatives, probabilités, priorités ou délais comparatifs.

À partir de ces classifications, l'IA peut aider à prioriser les menaces et les objectifs.

D = décider

Fonctions d'optimisation ressources/objectifs et menaces prioritaires.

Préparation du dérouler des actions.

On entre dans le domaine des sujets sensibles, la question centrale étant l'emplacement du curseur entre machine et humain…

A = Agir

La décision conduit à l'action… et donc au sujet de la conduite des opérations/Retex, par les humains seuls, par les humains assistés par l'IA, par l'IA supervisée par l'humain ou, encore par l'IA avalisée ou non par l'humain (rôle de vérification et de blocage éventuel). Tout ceci s'appliquant :

- à la généralisation des automatisations sur le champ de bataille, boucles courtes grâce à des outils IA localisés
- à l'augmentation du degré d'autonomie des plateformes et véhicules, notamment pour la logistique (approvisionnements, pleins, prévention des pannes, maintenance programmée…)

Une application phare potentielle est celle des essaims de drones aériens ou de robots d'assaut terrestres coordonnés, voire autocoordonnés. Cette nouvelle modalité d'action oblige à traiter la question des attaques à saturation/défense à saturation. Les outils IA arrivent ainsi au cœur de ces nouvelles modalités de combat et les systèmes d'armes létaux et autonomes (SALA), ou encore les munitions intelligentes, ne vont pas sans poser de sérieux problèmes de conscience aux armées des pays qui ont un certain sens de l'humain et de l'éthique.

Incidence sur l'organisation, les ressources humaines

Le paragraphe précédent a abordé l'incidence sur les opérations militaires, mais la vague de fond touche l'ensemble de l'organisation et du fonctionnement du système « défense »

La plus grande profondeur dans la compréhension de la situation stratégique, logistique et matérielle (durée de reste à vivre, HUMS — *Health and Usage Monitoring System* —, pour les

machines, pas pour les humains) peut être rapprochée partiellement du paragraphe opérations.

Surtout, l'IA bouscule les hiérarchies traditionnelles en déplaçant les niveaux de décision et les compétences nécessaires des différents échelons humains à l'intérieur des forces opérationnelles. Cela va-t-il imposer une nouvelle gestion des ressources humaines, avec les questions d'acceptabilité associées : nouveau rôle des chefs de groupe, S/O, Officiers ?

Se pose, enfin, pour les ressources humaines la question de la mise à niveau rapide et évolutive des compétences des spécialistes de tous les domaines classiques qui sont déjà modifiés ou vont être modifiés à court terme par l'arrivée des outils de l'IA…

Quand on aborde la question de l'architecture choisie pour un système donné, réflexion absolument indispensable, le positionnement de la place clef de la supervision (dans la réalité opérationnelle, plusieurs couches de supervision) est un facteur crucial : comment garder le contrôle si on délègue tout ou partie aux outils IA ?

De façon générale, l'IA est d'abord un outil d'optimisation, de classification, d'automatisation. Comment alors superviser des systèmes complexes intégrant de l'IA à tous les étages ? Il faut arbitrer entre ***Supervision/validations/allocation des ressources mémoires et énergies.***

C'est exactement le même type de problématique que l'on a rencontré depuis 2012 avec l'arrivée de l'IoT (Internet of Things = *Internet des objets*) : comment coordonner des millions, voire des milliards d'unités autonomes, avec quel partage de mémoire et de puissance de calcul ? Quelle forme et quels niveaux de validation (blockchains ?)

D'où une grande variété d'architectures, selon les arbitrages centralisation/décentralisation concernant les décisions et la supervision.

Une des solutions pratiques serait la maîtrise de ce qu'on appelle « les agents IA », ou encore l'« IA agentique », en supposant que les différents agents pourraient se coordonner dans un projet cohérent (?). Difficile, aujourd'hui, de faire la part entre « promesses marketing » et « réalité opérationnelle »…

Les questions de fond restent :

- l'homme dans la boucle, à quel endroit ? À quels niveaux tactiques/stratégiques ?
- peut-on accepter, localement, voire à d'autres niveaux, de retirer l'homme de la boucle ?
- simple « aide à la décision » ou bien « automatisation complète de telle ou telle fonction » ?

Cela devient encore plus compliqué lorsque l'on veut traiter des questions des systèmes embarqués, à cause des questions de sûreté et de risques humains.

Le SWOT de l'IA

S = forces

- Optimisation.
- Automatisation.
- Classification/priorisation des menaces et actions.
- Réactivité.
- Gestion de la complexité (essaims de drones ou munitions intelligentes, flottes logistiques et approvisionnements associés).

W = faiblesses

- Les taux d'erreurs, les biais et les hallucinations.
- Plus l'outil est spécialisé et entraîné sur des applications spécifiques, avec des bases d'apprentissage maîtrisées, plus l'IA considérée est fiable et moins sujette aux erreurs.
- Les possibilités des IA génératives ont donné l'idée à des utilisations dans le domaine de la programmation logicielle, mais les limites du *vibe coding* apparaissent rapidement : cela nécessite expertise et vérification par des « spécialistes ».
- *L'utilisation généralisée des outils IA ouvre un nouveau cycle de cybervulnérabilité avec l'*Introduction de nouveaux risques cyber, notamment :
  - les IA de reconnaissance de formes et de patterns sont facilement leurrées par des outils adverses (leurrage des reconnaissances d'image via des images truquées au niveau de certains pixels),
  - Si le corpus de règles est trop limité et la base d'entraînement trop normalisée (nettoyée) : pas de cas rares dans les références et le système

IA ne saura pas les reconnaître en situation opérationnelle (L'IA est hypermnésique, mais, jusqu'à preuve du contraire, n'invente rien).
- Management : un risque accru de micromanagement (perte d'efficacité, répercussion sur le moral des personnels…)

O = Opportunités
- Meilleure visibilité.
- Atténuation du brouillard de guerre.
- Amélioration de la discrimination des fausses informations, faux signaux télécoms et GPS (GPS Spoofing – leurrage –).
- Changements de doctrine ?
- Mise en œuvre de nouvelles technologies et concepts (attaques à saturation de drones…)
- Efficacité accrue de la bulle de protection aéro-terrestre, à l'image des développements récents RapidFire (canon antiaérien Thales KNDS) et Proteus (recyclage/rétrofit du canon de 20))

T = menaces
- Risque de compromissions dues à une mauvaise utilisation des outils IA, ou via des clouds non souverains ou des API *(application programming interface)* non sécurisés, ou par manque d'hygiène cyber des utilisateurs.
- Attaques ennemies à saturations, par drones tous milieux.
- SALA : comment garder le contrôle/risques de perte de contrôle avec les conséquences possibles de comportement inapproprié.
- Risques cyber spécifiques, liés à ces nouveaux outils IA.
- Management des personnels (opérationnels et administratifs) : risque de micromanagement, perte de sens, déstructuration des liens au niveau des ressources humaines.

Comment progresser

L'analyse SWOT met en évidence des faiblesses et différentes menaces, ce qui permet de cerner les voies de progrès.

Besoin d'une IA fiable et non biaisée

Cela se traite par la maîtrise des bases d'apprentissages et des réglages (validé par des experts académiques) et par l'hybridation avec des systèmes experts (ancrage dans le « réel »)

Besoin d'une IA de confiance pour la défense

À noter que ce besoin est parallèle à ceux pour l'aéronautique et la sécurité.

Tous nos grands systèmes de défense fonctionnent aujourd'hui avec PALANTIR/AZURE (Microsoft), AWS (Amazon), « en attendant mieux »…

Cette situation n'est pas tenable sur la durée, surtout si on prend en compte les risques de modification rapide des alliances stratégiques…

On ne peut que s'inquiéter du manque de constance et de cohérence de l'Europe sur ces questions d'industrie du numérique, il suffit d'évoquer les annonces faites sur la nécessité de construire un Cloud souverain et (relativement) indépendant dans l'espace européen, il y a seulement trois ans, volonté qui semble bien oubliée aujourd'hui…

En ce moment, au niveau mondial, se joue une course à la construction de centaines de Data Centers dédiés à l'IA, et au développement de la puissance de moyens de calcul spécifiques utilisables par l'IA militaire et la cryptographie (HPC — *High Performance Computing*)

Tous les grands acteurs ont compris qu'ils avaient besoin de supercalculateurs spécifiques pour une IA de défense.

L'Europe vient de commander un supercalculateur dédié à l'IA au français ATOS (installé en Allemagne), tandis que le ministère des Armées français a acheté un équivalent au tandem Orange (opérateur français) et HPE (fabricant américain)…

La question des capacités de calcul nécessaires pour soutenir le fort déploiement de l'IA dans le domaine de la Défense reste centrale. Sans puissance de calcul disponible, y compris avec des marges de réserve opérationnelle (pour faire face à une attaque massive à saturation), tout cela ne restera que théorique…

Conclusion

Tout le monde semble d'accord pour affirmer que le déploiement de tous ces nouveaux outils IA va augmenter **l'efficacité et la réactivité de nos forces** sur le champ de bataille ; même si

on peut exprimer des doutes sur la puissance des outils d'IA, on ne peut pas faire l'impasse sur ces nouveaux outils au niveau opérationnel.

Soyons conscients que cela introduit en même temps de nouvelles faiblesses potentielles et menaces, comme cela a toujours été le cas pour les nouveaux instruments du combat. Soyons aussi conscients que la mise en œuvre de ces outils va être d'une grande complexité, avec, notamment, beaucoup d'arbitrages humains à faire…

Cela pose parallèlement un défi capacitaire sérieux. Celui du développement indispensable d'une filière industrielle fiable et suffisamment autonome (cloud souverain, puissance de calcul instantané, composants critiques, équipes de conception des logiciels d'IA), française/européenne. Les grands opérateurs actuels sur lesquels reposent nos moyens peuvent faire défaut…

Les experts en cybermenaces donnent l'Europe largement dépassée par les États-Unis, eux-mêmes menacés par la puissance de frappe en IA de la Chine (qui a complètement rattrapé, voire dépassé, son retard initial en IA). La multiplication des cyberattaques contre les grands acteurs de Service et opérateurs publics par des agresseurs variés (des liens avec les services officiels de différents pays sont cités) en est la preuve affligeante.

D'où ces questions urgentes :

Quels plans d'investissements ? Quelles priorités ? Quels arbitrages budgétaires ?

Références

Documentation Web

Utilisation des IA génératives

L'effet ChatGPT : comment, en trois ans, l'IA a redéfini les recherches en ligne dans The Conversation

IA et transformation du travail

Pourquoi l'IA oblige les entreprises à repenser la valeur du travail dans The Conversation

Où et comment utiliser l'IA en entreprise ? Dans The Conversation.

C'est la question soulevée par l'économiste Caroline Gans Combe dans cet article. Le débat se focalise sur une liste d'emplois menacés de remplacement car « automatisables » ; mais ce critère est-il vraiment pertinent ? Les déboires du géant du conseil Deloitte montrent que non. Mandaté par le gouvernement australien, il a rédigé, avec l'IA, un rapport truffé de références académiques inexistantes et de citations inventées. Introduire l'IA au mauvais endroit peut coûter cher. Et d'autres secteurs ont subi les mêmes dérives. Alors, la vraie question n'est peut-être pas de déterminer ce qui peut être remplacé, mais où une telle substitution crée — ou détruit — de la valeur. Une réflexion qui nécessite une compréhension fine des tâches et de leur fonction stratégique dans les entreprises et une capacité des dirigeants à en saisir les points de fragilité.

IA, erreurs et hallucinations

Quand l'IA fait n'importe quoi, le cas du gratte-ciel et du trombone à coulisse dans The Conversation

IA et risques sécurité…

L'IA fait peser des risques sur la sécurité nationale, la démocratie et notre système de santé… Quelques pistes pour les réduire dans The Conversation

IA de confiance (particulièrement pertinente en matière de Défense)

Pour une IA de confiance | Thales Group

Documentation académique

J. Mattioli, Ch. Meyer. (2018) *L'Intelligence artificielle au service des systèmes critiques.* REE N° REE 2018-4, Dossier L'IA et l'industrie

J. Mattioli (2009), *Comprendre et choisir, les défis des systèmes d'information et d'aide à la décision.* Monographie SEE, Gestion de la

complexité et de l'information dans les grands systèmes critiques, CNRS Editions, janvier 2009, ISBN : 978-2-271-06828-6.

N. Museux, J. Mattioli, C. Laudy, H. Soubaras (2006). *Complex Event Processing approach for Strategic Intelligence.* In Proceedings 9th International Conference on Information Fusion, Fusion 2006.

J. Mattioli, F.-X. Josset. (2004) *A Viable Modelling Approach for Risk Assessment in Uncertain Environments. in Proceedings 10th International Conference on Information Processing and Management of Uncertainty in Knowledge*-Based Systems (IPMU 04), vol. 3, p. 1617-1624.

Domaines spécifiques

Proteus

Comment l'armée française a transformé de vieux canons des années 1970 en système anti-drones, Challenge (site payant)

https://www.challenges.fr/entreprise/defense/comment-larmee-francaise-a-transforme-de-vieux-canons-des-annees-1970-en-systeme-anti-drones□633182?fbclid=IwVERTSAO0dFhleHRuA2FlbQIxMABzcnRjBmFwcF9pZAwzNTA2ODU1MzE3MjgAAR4mr8Hr4soVJqyt8R5R□uVd□BBeTRuUt3sIfZNYKfu1nIGePtjyL9□3XWegWA□aem□ZNuNI8Ie4ybdk6W89jHInA&sfnsn=scwspmo

robots terrestres

Intelligence artificielle : vers une ère de robots soldats ? FranceInfo (17/12/2025 01:57

https://www.franceinfo.fr/internet/intelligence-artificielle/intelligence-artificielle-vers-une-ere-de-robots-soldats□7683868.html

écosystème industriel IA

NVIDIA et OPEN AI

: https://www.usine-digitale.fr/intelligence-artificielle/openai/intelligence-artificielle-amazon-est-en-passe-dinvestir-de-10-milliards-de-dollars-dans-openai.U7ZRJ7RHQNFLNEG3ZBTNDIDVQE.html

https://www.usine-digitale.fr/informatique/cloud/aws/intelligence-artificielle-aws-presente-ses-derniers-serveurs-equipes-de-puces-trainium3-pour-des-performances-4-fois-superieures.G4E2KCA6ZBE57DEN2MYTONOU7A.html

capacité chinoise de composants pour l'IA

https://www.clubic.com/actualite-592072-embargo-contourne-la-chine-possede-l-arme-technologique-qu-on-lui-refusait-dans-la-guerre-des-semi-condicteurs.html?fbclid=IwdGRzaAOxQWdleHRuA2FlbQIxMQBzcnRjBmFwcF9pZAwzNTA2ODU1MzE3MjgAAR49IjohIvYIUG□d8ysX3cgPD8pu7ZPQl8tsi4HpizeGnJeldQowlGCiBBeBsA□aem□dv11TGencoHw1lhbok5hhw

Intelligence artificielle générale

Interrogations

François Lefaudeux CHEAr SN16

Mais tout d'abord, qu'est-ce que l'intelligence artificielle générale ?

C'est aujourd'hui un objectif d'une partie importante de la communauté de l'IA, que ce soit dans sa composante académique ou dans sa composante commerciale (surtout dans la composante commerciale qui y consacre des ressources informatiques gigantesques).

En quoi consiste cet objectif ? Ni plus ni moins que de faire aussi bien si ce n'est mieux que l'homme dans tous les domaines. On n'est pas tout à fait dans le mythe de Prométhée ou dans l'ambition faustienne par l'ampleur du défi, mais pas loin. Avec, dans l'esprit, le risque que la comparaison aille jusqu'à la similitude de la chute…

Nous connaissons depuis quelques années l'essor de l'IA générative qui, parfois sans que nous nous en rendions compte ou fassions explicitement appel à elle, s'immisce dans de très nombreuses applications de notre quotidien sous des formes très variées. Cette IA générative a pour ambition de nous faciliter la vie (personnelle et professionnelle) en faisant pour nous pas mal de tâches, un peu comme le robot industriel a remplacé quasi totalement le Charlot du fim *Les temps modernes*. En évolution très rapide, elle va déjà plus loin dans différents domaines spécialisés où elle s'impose avec des performances surprenantes. Elle fait de la documentation scientifique ou technique de façon très exhaustive et avec une vitesse imbattable, elle sait écrire des lettres spécialisées, corriger votre style, proposer des rédactions alternatives (je ne l'ai cependant pas utilisée pour rédiger cet article à ma place, d'où, certainement, ses défauts perceptibles) et, bien sûr, elle est devenue imbattable aux échecs, elle est bonne dans l'interprétation des radiographies, elle conduit maintenant de manière plus sûre que l'homme, elle aide à trier les molécules ayant des possibilités d'action thérapeutique, etc.

Elle a aussi largement pénétré le domaine militaire, dont celui des armements. Elle sert ainsi à détecter les cibles dans le bruit des capteurs, à analyser les signaux, à mettre en œuvre des contre-mesures, à choisir des trajectoires. Elle intervient aussi massivement dans les bureaux d'études pour optimiser les conceptions matérielles et dans les centres de programmation pour aider à écrire rapidement du code applicatif.

L'IA générale promet, peut-être imprudemment, mais peut-être pas ! et ce, d'ici quelques années au plus, d'atteindre à un niveau la rendant indiscernable des meilleures performances humaines dans tous les domaines de l'esprit, voire même de la rendre discernable, car supérieure à toute intelligence humaine, individuelle ou collective.

Qu'entendre par « égale ou supérieure aux performances humaines ? Quels critères ? Quels tests de vérification ? Turing a abordé ce problème dans Computing Machinery and Intelligence [1] ou il décrit un test, depuis connu sous le nom de test de Turing, sensé trier ce qui a atteint la définition d'intelligence humaine de ce qui ne l'a pas atteint. Cet article facile à télécharger[2] est stupéfiant de prémonition. Turing a lui-même indiqué des limites de ce test — test dans lequel il s'agit pour un humain de démasquer une IA

1 *Mind* 49: 433-460.

2 Par exemple : https://informatique-fds.edu.umontpellier.fr/files/2021/11/Article-Turing-1950-236-433.pdf

cherchant à se faire passer pour un humain. Il écrit dans l'article déjà cité :

"I believe that in about fifty years' time it will be possible to programme computers, with a storage capacity of about 109, to make them play the imitation game so well that an average interrogator will not have more than 70 per cent chance of making the right identification after five minutes of questioning."

Un concours basé sur ce test a été régulièrement organisé de 1991 à 2019 par Hugh Loebner. Les machines passent depuis déjà longtemps haut la main ce test comme il l'avait pronostiqué, d'où l'arrêt du concours.

Tous les auteurs s'accordent pour dire que réussir ce test ne veut pas dire que la machine a l'intelligence de l'homme, encore moins les caractéristiques de l'humain, empathie, conscience, spiritualité, créativité (imagination), irrationalité, orgueil, etc., toutes notions qui ont un sens, mais sont difficiles à quantifier ;

Turing était conscient des limites de sa définition d'intelligence artificielle et il avait abordé, justement, le thème de la conscience ; ainsi, toujours dans le même article :

" I do not wish to give the impression that I think there is no mystery about consciousness. There is, for instance, something of a paradox connected with any attempt to localise it. But I do not think these mysteries necessarily need to be solved before we can answer the question with which we are concerned in this paper."

Pour ce qui concerne la localisation, l'âme est encore plus difficile à localiser, mais je sors, là, du sujet.

L'Académie des technologies a, repris, il y a une quinzaine d'années, le thème de la conscience et des tests qui permettraient d'attribuer ou non à la machine cette qualité, sans conclure[3].

Je n'irai pas beaucoup plus loin sur la question du sens à donner à « semblable à l'homme », le sujet devenant rapidement plus du domaine de la philosophie que de celui de la science. Ainsi, l'homme a manifestement un fond irrationnel difficile à expliciter algorithmiquement, et dont la transposition aux « *discrete state machines* » ne paraît pas techniquement évidente, outre de ne pas être a priori souhaitable.

La notion d'intelligence artificielle générale a donc ses limites, mais, même dans le cadre de ces limites, l'ambition est grande et les conséquences potentiellement immenses.

Je ne m'attarderai pas sur les dimensions philosophique et religieuse, me limitant à en esquisser le paysage. L'homme s'est décrit comme étant à l'image de Dieu et au centre du créé. Première crise importante, Copernic réfutant l'hypothèse que la Terre, et donc l'homme qui l'habite, soit le centre du monde, centre autour duquel tous les autres astres tourneraient, le soleil ainsi que la sphère des fixes (la limite de l'Univers sur laquelle sont collées les étoiles) et proposant de placer le soleil comme centre (et de ce fait reléguant la Terre au rang de planète banale au même titre que Venus, Mars, etc.).

Giordano Bruno va, un peu plus tard, beaucoup plus loin, puisqu'il pense multitude de « mondes », soit, dans son langage, de systèmes du genre système solaire comportant donc des planètes potentiellement habitées. Il a fini brûlé, mais l'Église a dû, longtemps après, accepter les idées copernicienne et galiléenne, elle a même sorti les œuvres de Giordano Bruno de l'index (elle y a mis le temps : 1835, plus de deux siècles).

La prétention des développeurs de l'IA générale est d'une tout autre envergure, car si, tel Frankenstein[4], ils arrivent à construire ce surhomme, si donc la machine devient égale ou supérieure à l'homme, se pose immédiatement la question : l'homme n'est-il qu'une machine ? Ceci explique l'inquiétude explicitée par plusieurs acteurs de l'IA, inquiétude qui s'exprime par la

3 Ainsi, l'Académie des technologies a réfléchi à cet aspect. Voir *Vers une technologie de la conscience* EDP Sciences 2013

4 Le héros de Mary Wollstonecraft Shelley dans son *Frankenstein* (1816) est un robot humanoïde (ou assimilable à un hybride homme-machine ? il a tout du surhomme) qui se retourne contre son imprudent créateur et le poursuit partout dans le monde.

question : l'IA générale ne risque-t-elle pas de conduire à la fin de l'homme ?

L'argument selon lequel l'homme est imprévisible, non rationnel et autres défauts qui le distingueraient de la machine n'est pas recevable : il revient à dire que l'homme serait non seulement une machine, mais, en plus, une mauvaise machine ! D'ailleurs, pour les tests comparatifs d'intelligence, les concepteurs d'IA ont introduit des comportements erratiques très programmés, pour ne pas se montrer trop différents de l'homme !

On ne peut empêcher l'IA générale de se développer et on ne pourra pas l'interdire ni globalement ni même, probablement, dans les quelques domaines jugés les plus problématiques, d'un simple trait de plume, ceci malgré les inquiétudes des acteurs de l'IA eux-mêmes (voir annexe). L'esprit de conservation le plus élémentaire impose donc de s'y préparer, même si on peut encore avoir quelques doutes sur la puissance qu'atteindra ce nouvel outil.

Le champ des domaines applicatifs est très vaste, même en se limitant à ce qui touche à l'art de la guerre. Je n'ai donc d'autre choix ni d'autre ambition que de présenter quelques illustrations.

Après avoir beaucoup procrastiné, les armées des grands pays ont basculé vers l'utilisation des petits drones aériens dans les opérations locales. La guerre en Ukraine a précipité le mouvement, d'abord comme moyen d'observation, ensuite comme vecteur d'arme. Le champ d'évolution le plus important est celui du pilotage et de l'autonomie de ces drones. D'abord téléopérés, le développement des contre-mesures a imposé de les rendre de plus en plus autonomes et, donc, de les doter d'une IA qui va se perfectionnant de jour en jour. Est-on toujours dans le domaine de l'IA générative ou se rapproche-t-on de la notion d'IA générale ? On est, plus pragmatiquement, dans le domaine de l'appréciation du sens à donner aux mots. On arrive avec les drones rôdeurs dans le domaine de l'autonomie de décision quasi complète de ces engins. Certes, les armes « *fire and forget* » existent depuis longtemps, mais il y a différence de nature : l'arme *fire and forget* est tirée contre une cible identifiée, alors que le drone part avec une simple consigne du genre « si tu vois quelque chose bouger ressemblant à un humain, à un camion, à un char, etc., tire ». Les mines étaient jusqu'à présent les seules armes totalement autonomes, bien loin de l'IA[5], mais immobiles (dans le domaine naval, les mines dérivantes sont interdites depuis très longtemps).

Les robots terrestres, en cours de développement rapide, sont pour l'instant, et pour autant que je sache, un peu moins avancés du point de vue autonomie, mais nul doute qu'ils acquerront rapidement le degré d'autonomie des drones aériens rôdeurs, et seront lancés avec comme consigne « avance dans telle direction et tire sur tout ce qui à l'air d'un homme qui bouge (et porte une arme) en face de toi », 'et porte une arme' entre parenthèses, car je doute que certains pays s'imposent ce caveat complexe (le mot lui-même est un peu laborieux dans certaines langues — Предостережение)..

Les drones navals constituent un domaine un peu particulier en raison des distances et surtout des temps mis en œuvre, et, de plus, des problèmes posés par l'opacité radioélectrique du milieu pour les drones sous-marins[6].

Cette évolution robotique des armes et des vecteurs d'armes constitue un changement plus radical qu'il n'y paraît à première vue du paradigme de la guerre qui était depuis l'antiquité le monopole du bras armé, le fut-il d'une lance. L'arme, aujourd'hui, n'a plus besoin du bras qui la tient, ni même d'un bras virtuel (et de la conscience qui le maîtrise) pour agir.

L'étape suivante, que l'on peut sans doute qualifier de première mise en œuvre dans le

5 À l'exception des mines torpilles dont la consigne était et reste « Si un navire ayant telles ou telles caractéristiques passe à portée, tire ».

6 L'attaque récente par drone naval submersible ou semi-submersible (quoi d'autre ?) d'un sous-marin russe à quai à Novorossiïsk, interpelle cependant, vu les protections sérieuses de l'entrée de ce port.

domaine militaire de l'IA générale, est celle des meutes de drones (aériens, terrestres, navals), organisés en troupe constituée, avec une intelligence centralisée ou répartie, autonome, au plus supervisée de plus ou moins loin (probablement de manière lointaine et lâche) par une conscience humaine.

Le modèle archétypique de meutes de drones travaillant de manière coopérative est l'équipe de joueurs de football, thème de nombreux laboratoires avec concours interéquipes, comme les concours d'échecs entre IA (l'étape des concours entre IA et joueurs humains est dépassée), continuent d'être une vitrine des progrès de l'IA spécialisée. L'enjeu du modèle de l'équipe de football est celui de la maîtrise de l'intelligence collective, le « douzième cerveau ». La recherche va donc dès aujourd'hui au-delà du concept de l'avion de chasse piloté, « leader » d'une escadrille de drones de combat, même si ce concept d'escadrille n'est pas encore à un TRL très élevé et va demander encore pas mal de travail pour aboutir concrètement de manière utile. Mais les avancées se succèdent à un tel rythme dans le domaine de l'IA, que les auteurs de science-fiction eux-mêmes sont en passe d'être dépassés !

Dans le domaine du combat terrestre, l'armée de robots coopératifs, humanoïdes ou non — la question n'est pas là —, aussi nombreuse que l'armée de guerriers d'argile de l'empereur 秦始皇 (Qin Shi Huang) n'est plus une utopie, mais une hypothèse concrète à prendre en compte. De telles armées verront normalement leurs objectifs stratégiques fixés par des états-majors extérieurs, encore humains dans un premier temps ; mais l'exécution, voire la conception, de la manœuvre tactique et son évolution en fonction des mouvements adverses, seront à terme laissées à l'intelligence répartie de cette troupe. De plus, les états-majors humains qui définissent les objectifs et les modalités de la manœuvre stratégique s'appuient déjà sur l'intelligence artificielle pour quantifier les scénarios, les comparer, et, finalement, choisir la manœuvre apparaissant la plus favorable. Les officiers d'état-major eux-mêmes, ne risquent-ils pas d'être à terme marginalisés ?

L'impact de l'IA générale dans le domaine naval est plus difficile à cerner. J'ai, personnellement, du mal à imaginer un porte-avions robotisé, mettant en œuvre des flottilles d'aéronefs eux-mêmes totalement robotisés, ceci pendant des mois et à des milliers de kilomètres de leur base. Pour ce qui concerne le sous-marins, le CPE à ses débuts sous la houlette d'Hugues de l'Estoile, avait, je crois, lancé l'étude d'un sous-marin autonome, mais, en fait, lié en permanence à ses opérateurs en surface, donc finalement un drone classique sans autonomie de décision significative. Aller au-delà ? Les Ukrainiens avec leur attaque récente déjà citée sont peut-être sur cette voie…

Depuis longtemps, dans les domaines aérien et naval, il n'y a pas contact direct entre humains, tout se passe « à distance ». Dans le combat terrestre, au contraire, les opérations comportent le plus souvent encore des phases de combat rapproché. C'était toujours quotidiennement le cas en Ukraine en 2022 et 2023 où on se battait de porte à porte. C'est avec la généralisation des drones rôdeurs de moins en moins le cas ; il y a encore des hommes en première ligne, parfois, comme durant la Première Guerre mondiale, à faible distance les uns des autres, protégés dans des tranchées couvertes, mais toute tentative d'assaut à découvert est quasi suicidaire. Comment imaginer dans un avenir proche des combats mixtes humains-robots (avec plusieurs configurations : armée de robots contre une armée d'humains ou, de chaque côté, armées mixtes composées d'humains et de robots), comment dans une unité mixte imaginer le partage de la décision entre robot et humain ? Comment le groupe de robots en intelligence partagée communiquera-t-il avec les humains du groupe, qui aura le plus de poids dans les choix tactiques ? Toutes ces questions, et bien d'autres sont des questions ouvertes… Et tout ceci souvent en milieu urbain avec des populations restées sur

place, otages de la situation ? On peut essayer de se rassurer en avançant le fait que le robot peut toujours être immédiatement bloqué via le gros bouton rouge « arrêt d'urgence » qui coupe son alimentation électrique, mais, même cela est-il vrai si plusieurs centaines de robots se coordonnent dans un réseau d'intelligence partagée ?

Va-t-on finalement vers le combat d'armées de robots sans présence humaine ?

De manière très globale, la victoire militaire résulte depuis les temps les plus anciens de la coopération fructueuse entre le soldat, le bras armé, et le forgeron qui fournit l'arme. C'est la coopération entre Mars et Vulcain. Ce sont les deux faces du même Janus. Cette coopération étroite restera encore certainement encore pour quelque temps la condition *sine qua non* de forces armées efficaces. L'homme armé dans la guerre est décisif, mais, depuis le silex taillé, son armement a crû en importance, ne serait-ce qu'en matière de financement. Ce mouvement s'est accéléré depuis les débuts de l'ère industrielle, l'IA ne peut qu'accélérer encore le mouvement. Si l'homme doit rester et restera certainement largement, mais pour combien de temps, au centre de la boucle, cette boucle, déjà très technique, va le devenir bien plus encore. De nombreuses questions se posent auxquelles il faut absolument se préparer à répondre (et il faudrait même avoir déjà répondu clairement à certaines).

La question de l'existence de l'homme en armes ou de son remplacement partiel et progressif par le robait doté d'intelligence est plus que jamais fondamentale, ceci pour deux raisons, la première technique : le soldat prend du temps pour être formé, plusieurs années pour un pilote de chasse, cas proche du maximum, et, en poussant le cynisme, préalablement vingt ans à fabriquer ! La seconde psychologique : l'espace européen n'a pas vu la guerre de haute intensité depuis quatre-vingts ans, personne n'est réellement prêt à, de nouveau, donner sa vie pour la Patrie ou voir ses enfants ou petits-enfants mourir pour elle ; ceci évoluera peut-être, mais il y faut du temps. Ce double constat, combiné avec l'entrée en lice d'une IA de plus en plus générale, pousse encore plus à « automatiser » le champ de bataille et, donc, à faire reposer la guerre et la recherche de la victoire encore plus sur Vulcain…

Mais Vulcain reste-t-il la bonne référence ? En effet, si, certes, la composante physique des armes reste centrale, et donc la forge, les composantes immatérielles des armements prennent une place de plus en plus majeure, de même que les éléments immatériels de la guerre, contre-mesures électroniques et informatiques, cyberguerre, guerre des réseaux sociaux, action psychologique utilisant tous les moyens techniques à disposition, prennent chaque jour une place plus importante.

Pour ce qui concerne les matériels, intelligence artificielle ou non, l'expérience des deux grands conflits mondiaux du XXe siècle, confirmée par le déroulement du conflit ukrainien, montre que la montée aux extrêmes théorisée par Clausewitz est aujourd'hui pour une part significative celle de la production industrielle. Le temps de paix distingue les consommables (munitions, carburants) et les investissements (véhicules, canons…) Dans la guerre de haute intensité (clausewitzienne pourrait-on dire), tout entre dans la catégorie « consommables ». Les forces russes ont perdu en Ukraine des milliers de chars, les Ukrainiens doivent être réapprovisionnés en permanence en systèmes d'armes pour faire face à leur attrition très rapide, et, lorsqu'il n'y pas attrition, il faut faire face à l'usure accélérée (pour prendre un exemple d'armement français, les canons Caesar ukrainiens tirent sans doute par jour au moins autant que les systèmes français tirent par an en entraînement et les tubes doivent être remplacés bien plus souvent). Pour ce qui est des consommables traditionnels, comme les munitions, le caractère cyclique temps de paix/temps de guerre est lui aussi très difficile à gérer, vu l'ampleur de l'écart entre étiage et crue. Une analyse récente montrait que les

efforts combinés des industries d'armement américaines et européennes ne parvenaient pas (ou ne parviendraient pas même sans le blocage actuel par la présidence américaine), à satisfaire, les stocks étant pratiquement épuisés, aux besoins de l'artillerie de 155 ukrainienne. De nombreuses caractéristiques obligent à distinguer les industries civiles des industries de défense, celle de l'amplitude des cycles, jointe à l'obligation de monter rapidement en cadence après une longue période de léthargie en est une importante. Enfin, sur ce sujet de l'industrie, éloigné du thème central de cet article, à noter que l'évolution très rapide, dans les mois précédant le déclenchement d'un conflit important et, encore plus, les premiers mois des hostilités (rien, jamais, ne s'y passe comme prévu) des types de besoins et des technologies employées, rendent difficile la gestion d'un outil industriel adapté à ces contraintes drastiques.

Si on va vers des guerres de plus en plus robotisées, la supériorité, théorique, ne reposera plus sur le ratio du nombre d'hommes, mais sur celui de la capacité de production des robots. Mars s'effaçant devant Vulcain…

Je reviens à l'industrie immatérielle, elle est certes aussi une industrie de moyens : centres de calculs puissants, mais comme c'est le plus souvent le cas en informatique, l'outil peut indifféremment traiter du besoin militaire et du besoin civil. Encore faut-il avoir accès à des moyens non vulnérables et ne pouvant être soumis à des embargos. On retrouve ici le thème de la souveraineté numérique… L'essentiel reste cependant les hommes. Ironie, ils sont absolument indispensables pour faire progresser l'IA militaire et adapter très rapidement les logiciels des armements, qu'ils soient à base d'IA ou d'algorithmie classique, défensivement aux changements logiciels de l'adversaire ou pour trouver, face offensive du sujet, des moyens nouveaux de pénétrer les défenses de l'adversaire, qu'il s'agisse des défenses matérielles ou de celles du monde cyber…

Parallèlement, s'interroger sur l'ensemble des implications du passage de l'IA de générative à générale est une nécessité. Il faut, j'en suis persuadé, prendre au sérieux la mise en garde qui figure en annexe, notamment concernant le risque pour la survie de l'humanité. Je vois ce risque comme plus grand que celui de l'armement nucléaire, car sans seuil et donc sans possibilité simple de mise en place d'une doctrine de dissuasion du genre MAD.

Annexe — Appel à un moratoire sur la superintelligence

Appel en date du 24 octobre 2025 lancé par environ huit cents scientifiques et autres personnalités, pour stopper la course à une « superintelligence », tant que les problèmes éthiques et de société que de tels développements pourraient créer ou accentuer n'ont pas été abordés au fond.

Le « statement » est ultra court :

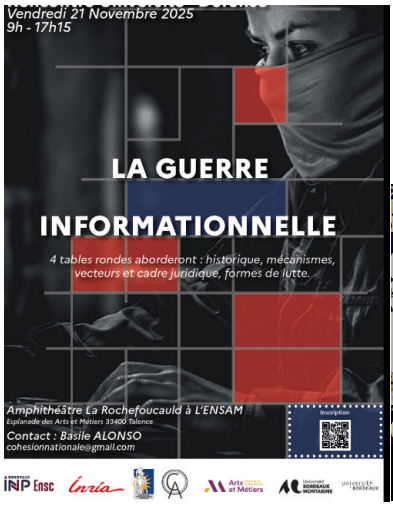
We call for a prohibition on the development of superintelligence, not lifted before there is

1. **broad scientific consensus that it will be done safely and controllably, and**
2. **strong public buy-in.**

La note de contexte qui l'introduit est un peu plus explicite et manifeste une inquiétude profonde (extinction possible de l'humanité) :

Context: Innovative AI tools may bring unprecedented health and prosperity. However, alongside tools, many leading AI companies have the stated goal of building superintelligence in the coming decade that can significantly outperform all humans on essentially all cognitive tasks. This has raised concerns, ranging from human economic obsolescence and disempowerment, losses of freedom, civil liberties, dignity, and control, to national security risks and even potential human extinction. The succinct statement below aims to create common knowledge of the growing number of experts and public figures who oppose a rush to superintelligence.

On est, évidemment, dans le domaine de l'utopie ou de la lettre au Père Noël, mais la preoccupation est légitime tant dans le domaine civil, qui est celui de cette intervention publique, que dans le domaine militaire.



Journée guerre informationnelle 21 novembre 2025 à Bordeaux

Norbert Laurençon

Contexte

Cette journée a été réalisée dans le cadre des rencontres université-défense qui se tiennent chaque année à Bordeaux ; après un discours préliminaire de l'officier général de la zone de défense et de sécurité,sud (OGZDS), le général Groen qui a rappelé les principales attaques informationnelles subies ces dernières années (Charnier de Gossi au Mali, punaises de lit et invasion de rats à Paris, étoiles de David, tentatives d'influence électorales, déstabilisation du Président français à travers ses proches) quatre tables rondes sur les sujets :

1. historique et genèse de la guerre de l'information ;
2. mécanismes et stratégies mises en œuvre ;
3. vecteurs et outils utilisés ;
4. cadre juridique et formes de lutte ;

ont suivi.

Principaux éléments de ces tables rondes

Deux définitions et constations préalables :

- la guerre informationnelle est l'usage offensif ou défensif de l'information — sa production, sa manipulation, sa diffusion ou son blocage — afin d'influencer les perceptions, les décisions et les comportements d'un individu, d'un groupe ou d'un État :
- dans le domaine des entreprises et des organisations, l'intelligence économique (IE) constitue l'arme la plus efficace pour gagner cette guerre de l'information qui prend aujourd'hui une place de plus en plus grande dans les conflits, mais aussi dans toutes les compétitions qui se créent.

On peut définir la guerre informationnelle comme étant l'ensemble des actions coordonnées de **collecte**, **analyse**, diffusion et **protection** de l'information stratégique au service d'une organisation (entreprise, institution, État) pour améliorer sa compétitivité et soutenir sa prise de décision.

Une opération d'influence comporte habituellement trois composantes qui peuvent faire évoluer la compréhension d'un individu :

- la première partie touche généralement la logique, la connaissance des personnes visées. Exemples Airbus/Boeing : Nombre d'avions livrés/commandés… chaque année ;
- la deuxième partie touche l'affectif avec un narratif de récits : exemple : insistance de Boeing sur l'appartenance à une grande nation depuis les origines de celle-ci, d'Airbus sur la réussite d'une intégration européenne, l'innovation, le dynamisme,
- la démonstration d'une meilleure sécurité et d'un meilleur confort.
- la troisième partie touche le cognitif : amener les individus à conclure, pensent-ils d'eux-

mêmes, qu'ils ne peuvent pas prendre des avions soit d'Airbus soit de Boeing. Ceci correspond à un affectif amplifié afin de saturer les cerveaux et de couper la réflexion (Exemple sponsoring des États présenté comme source d'Illégalité).

Les guerres informationnelles actuelles ont, en particulier, pour but de déstabiliser des États, voire la démocratie occidentale toute entière.

- attaque de la science (La vérité scientifique gêne l'influence) ;
- impossibilité de se baser sur le droit, du fait de la structure même des réseaux sociaux qui ont changé le mode de diffusion et de maîtrise de l'information en passant de rumeurs et de récits globalement maîtrisés par les États à la possibilité pour une personne de déstabiliser ou d'orienter toute une population de façon ouverte (Ex : Elon Musk) ou anonyme avec une force cachée (trolls).

NB : Avec humour une intervenante a proposé la création d'un ministère de la Vérité ce qui Illustre bien la situation actuelle.

En utilisant le numérique, les guerres informationnelles peuvent toucher toutes les dimensions d'un conflit en se glissant dans l'hybridité de ces conflits, et ceci au niveau mondial, en utilisant divers types de supports tels que les images, le narratif ou la structure même de notre mode de pensée

Comme dans toutes les évolutions techniques et sociétales rapides, la loi ne peut pas suivre la vitesse des changements en cours, ce qui pose d'autant plus de problèmes.

En conclusion, on peut dire que la guerre informationnelle est un outil puissant pour déstabiliser une nation sans l'emploi des armes conventionnelles, mais peut être avec autant d'efficacité quant au résultat final.