

L'intelligence artificielle au prisme des affaires militaires américaines

Autor(en): **Ventre, Daniel**

Objekttyp: **Article**

Zeitschrift: **Revue Militaire Suisse**

Band (Jahr): - **(2021)**

Heft 1

PDF erstellt am: **27.09.2024**

Persistenter Link: <https://doi.org/10.5169/seals-977657>

Nutzungsbedingungen

Die ETH-Bibliothek ist Anbieterin der digitalisierten Zeitschriften. Sie besitzt keine Urheberrechte an den Inhalten der Zeitschriften. Die Rechte liegen in der Regel bei den Herausgebern.

Die auf der Plattform e-periodica veröffentlichten Dokumente stehen für nicht-kommerzielle Zwecke in Lehre und Forschung sowie für die private Nutzung frei zur Verfügung. Einzelne Dateien oder Ausdrucke aus diesem Angebot können zusammen mit diesen Nutzungsbedingungen und den korrekten Herkunftsbezeichnungen weitergegeben werden.

Das Veröffentlichen von Bildern in Print- und Online-Publikationen ist nur mit vorheriger Genehmigung der Rechteinhaber erlaubt. Die systematische Speicherung von Teilen des elektronischen Angebots auf anderen Servern bedarf ebenfalls des schriftlichen Einverständnisses der Rechteinhaber.

Haftungsausschluss

Alle Angaben erfolgen ohne Gewähr für Vollständigkeit oder Richtigkeit. Es wird keine Haftung übernommen für Schäden durch die Verwendung von Informationen aus diesem Online-Angebot oder durch das Fehlen von Informationen. Dies gilt auch für Inhalte Dritter, die über dieses Angebot zugänglich sind.



Cyber

L'intelligence artificielle au prisme des affaires militaires américaines

Daniel Ventre

Docteur en Science Politique, chercheur au CESDIP (Centre de Recherche sur le Droit et les Institutions Pénales, UMR 8183), CNRS.

L'intelligence artificielle est née dans les années 1950 aux Etats-Unis de la convergence de plusieurs disciplines (...). Les recherches se sont rapidement développées peu après, dès le début des années 1960 dans d'autres pays, aujourd'hui acteurs majeurs du domaine : Russie, en Chine, Japon, France...

Le parcours de l'IA ne fut pas linéaire. On peut découper cette chronologie comme suit :

- Une première phase de 1956 à 1970, qualifiée de premier « printemps » de l'IA, au cours de laquelle les pionniers de l'IA, optimistes, estiment pouvoir atteindre leurs objectifs (créer une intelligence artificielle dont les capacités viendraient concurrencer celles du cerveau humain en tous domaines) dans les 25 années à venir. Mais les progrès sont moins rapides que prévu, et les soutiens financiers se font plus rares ;
- La décennie suivante, 1972-1982, serait alors le premier « hiver » de l'IA. La recherche se poursuit mais fait face à une diminution des crédits ;
- La période 1982 - 1987 est celle d'un bref renouveau, sous l'impulsion du programme japonais pour une nouvelle génération d'ordinateurs ;
- Entre 1987 et 2010 le marché de l'IA est à la peine ;
- A partir de 2010, l'IA connaît un nouvel élan, porté par la conjonction de plusieurs technologies qui ouvrent de nouvelles perspectives : le *big data*, le *machine learning*, le *cloud computing*.

Depuis lors les Etats et le secteur privé investissent massivement dans l'IA. Les promesses d'avancées scientifiques et technologiques rapides aux impacts majeurs sur la société ont politisé l'enjeu. « L'intelligence artificielle transforme la nature de presque tout ce qui est lié à la vie humaine, par exemple l'emploi, l'économie, la communication, la guerre, la vie privée, la sécurité, l'éthique, la santé, etc. »¹. Nombreux sont les Etats qui

dans le monde se sont dotés ces dernières années de « stratégies nationales pour l'Intelligence Artificielle », essentiellement depuis 2015.

On y construit ou anticipe une société moderne hyper-connectée (monde réticulaire, monde d'objets communicants, cyberspace porté à l'extrême de ses possibilités) et robotisée, dans laquelle l'IA jouera un rôle majeur. Ce triptyque « cyber-robotique-IA » est central. De sa maîtrise les Etats veulent construire leur puissance à la fois économique et politique, mais aussi militaire, et l'imposer sur la scène internationale.

L'IA dans le champ militaire L'IA et les forces de défense américaines

Les affaires militaires, l'art de la guerre, les enjeux de sécurité et de défense sont emportés dans cette dynamique. La relation qu'entretiennent les forces de défense avec la R&D en IA s'est nouée aux premières heures de la discipline. Aux Etats-Unis, l'ARPA fut l'un des principaux financeurs des travaux menés à Stanford ou au MIT. Au cours des décennies qui se sont depuis écoulées, la défense américaine a porté plusieurs projets successifs pour tenter de créer des machines intelligentes (c'est-à-dire autorisant de véritables interactions entre l'homme et la machine, la machine et son environnement, et de concevoir des machines autonomes). Rappelons par exemple les ambitions de la DARPA inscrites en 1983 dans un plan² pour la conception de nouvelles générations de calculateurs : le projet visait à combiner les progrès de l'IA, de l'informatique et de la micro-électronique pour parvenir à cet objectif. Plus près de nous, en 2017, le Département de la Défense américain a initié le projet MAVEN AI, consistant en l'exploitation des capacités du machine learning pour identifier dans des milliers

1 Amit Tyagi, *Artificial Intelligence: Boon or Bane?*, 16 pages, 2016, <https://dx.doi.org/10.2139/ssrn.2836438>

2 DARPA, *Strategic Computing, New-Generation Computing Technology. A strategic plan for its development and application to critical problems in defense*, 28 octobre 1983, Etats-Unis.

Titre du document	Pays	Auteur	Année
Artificial intelligence: opportunities and implications for the future of decision making	Royaume-Uni	Government Office for Science	2015
Three -Year Guidance for Internet Plus Artificial Intelligence Plan (2016-2018)	Chine	Gouvernement	2016
The national artificial intelligence research and development strategic plan	Etats-Unis	National Science and Technology Council. Networking and Information Technology Research and Development Subcommittee (NITRD)	2016
Pan-Canadian artificial intelligence strategy	Canada	CIFAR, finance par le gouvernement canadien, Facebook et la RBC Foundation	2017
Artificial Intelligence Technology Strategy	Japon	Report of Strategic Council for AI Technology	2017
AI Singapore	Singapour	Gouvernement	2017
Artificial Intelligence strategy	Allemagne	The Federal Government	2018
FranceIA Strategy	France	Agoranov, Secrétariat d'Etat à l'Innovation, Secrétariat d'Etat à l'enseignement supérieur et la recherche	2018
National Strategy for Artificial Intelligence	Inde	NITI Aayog	2018
Stratégie nationale	Russie	Gouvernement	2019

Tableau : quelques documents officiels introduisant les stratégies nationales en matière d'IA

d'heures de vidéos enregistrées par les drones, objets et individus. Le projet s'inscrit dans la cadre de la guerre contre l'Etat Islamique. Le projet est réalisé par une équipe créée spécifiquement: l'AWCFT (Algorithmic Warfare Cross-Functional Team). Le secrétaire à la Défense³ rappelle à cette occasion ce que les armées attendent de cette initiative: « l'objectif de l'AWCFT es de transformer l'énorme volume de données dont dispose le Département de la Défense en renseignement exploitable et en connaissance en temps réel ». Les moyens développés doivent répondre aux besoins opérationnels immédiats. La stratégie américaine consiste à progresser très rapidement, et pour cela choisit de privilégier les partenariats avec le secteur privé (l'entreprise Google fut par exemple appelée à contribuer au projet MAVEN), et de militariser des produits commerciaux existant.

Le Département de la Défense américain a publié récemment (en 2018) sa stratégie pour l'intelligence artificielle⁴. Le texte pourrait être résumé en son message central: les forces de défense doivent s'appropriier l'IA aussi rapidement que possible (le document insiste à plusieurs reprises sur la nécessité d'accélérer, d'aller vite, etc.) afin de ne pas être prises de vitesse par les autres grandes nations qui toutes se sont lancées dans cette nouvelle forme de course technologique et à l'armement (Russie, Chine, pays européens, etc.) Au sein du Département de la Défense, a été créé en 2018 le Joint

Artificial Intelligence Center (JAIC),⁵ centre d'excellence spécifique qui viendra compléter les actions de la DARPA et autres laboratoires de recherche militaires américains. Sa principale fonction est d'identifier les applications possibles de l'IA, apprécier leur potentiel, les tester, développer, et mettre en œuvre, dans des projets à moyen et long terme. On voit bien que l'enjeu est d'opérationnaliser les avancées de la science. Les efforts se concentrent sur des systèmes d'aide à la décision (extraction d'information dans des masses de données sons et images; outils d'aide à l'analyse des multiples options dans le champ de la prise de décision au niveau des commandements), accroître la sûreté et sécurité des systèmes d'armes dans des environnements où les conditions changent rapidement; systèmes prévisionnels aidant à la gestion des flux d'approvisionnement et de la maintenance des équipements, et globalement alléger la charge de travail de l'homme. Bien entendu les forces de défense œuvrent au développement d'armes dotées d'IA, autonomes ou semi-autonomes.

L'IA et ses applications militaires

L'ouvrage de Manuel de Landa, « War in the age of intelligent machines »⁶ (1991) propose une lecture prospective du potentiel de l'IA dans la guerre, transformée par l'irruption des machines intelligentes. L'auteur envisage la présence de deux catégories d'IA dans les armées: celle qui assiste le militaire, le libère de tâches routinières ou lui apporte une aide à la décision; et celle qui réalise, exécute, agit, prend des décisions. La première

3 Mémoire du Secrétaire à la Défense, 26 avril 2017, Etats-Unis.

4 U.S. Department of Defense, Summary of the 2018 Department of Defense Artificial Intelligence Strategy, 17 pages, 2018, <https://media.defense.gov/2019/Feb/12/2002088963/-1/-1/1/SUMMARY-OF-DOD-AI-STRATEGY.PDF>

5 <https://dodcio.defense.gov/About-DoD-CIO/Organization/JAIC/>

6 Manuel de Landa, War in the Age of intelligent machines, MIT Press, New York, 1991

maintient l'homme dans la boucle, la seconde tend à le mettre à l'écart en se substituant à lui. Toutefois, selon lui, on ne saurait envisager des robots semblables aux humaines, qui remplaceraient les soldats sur le théâtre d'opérations, ou des robots qui assureraient les fonctions de commandement. On se dirigerait plus probablement vers des applications traditionnelles de l'informatique ou de l'ordinateur dans la guerre, augmentées par l'IA. Mais l'introduction de l'IA dans la guerre aura des effets sur celle-ci. Le recours aux armes autonomes permettra non seulement d'éloigner l'homme du feu de l'ennemi, mais aussi d'écartier le soldat de la boucle décisionnelle (dès lors que c'est la machine qui, dans le feu de l'action, décidera et agira). La réflexion semble axée sur le juste équilibre qu'il conviendra de trouver entre mise à l'écart de l'homme et association plus étroite entre l'homme et la machine.

Les développements de l'IA militaire au cours des années à venir devraient concerner les domaines suivants⁷ :

- Les plates-formes de combat (IA embarquée dans les armes notamment, systèmes de combat moins dépendants de l'action humaine, armes autonomes capables de mener des attaques de manière collaborative);
- La cybersécurité;
- La logistique et les transports: l'utilisation de l'IA pourrait permettre d'optimiser ces fonctions, de réduire les coûts, raccourcir les délais, détecter les anomalies, gérer par plus grande anticipation;
- La reconnaissance de cible;
- La médecine sur le théâtre d'opération;
- Les outils de simulation de combat et d'entraînement;
- Le monitoring des menaces et analyse de la situation s'appuient sur des opérations d'ISR qui peuvent mobiliser des équipements dotés d'IA (drones de surveillance);
- Le traitement de l'information (information processing), segment qui devrait par ailleurs dominer le marché de l'IA militaire au cours des prochaines années. C'est en Chine que la croissance de ce marché devrait être la plus marquée.

L'IA dans la cyberdéfense: quels enjeux, quels acteurs, quelles applications?

Nous considérons pour notre part l'IA comme une nouvelle brique du cyberspace, dont elle contribue à étendre l'emprise sur le monde. Paradoxalement, nous constatons l'absence de toute référence à l'intelligence artificielle dans un document clef de la stratégie du cyberspace du Département de la Défense américain, qu'est la Joint-Publication JP 3-12 « Cyberspace Operations ». Dans sa version de 2018,⁸ l'intelligence artificielle est absente. La version de 2013⁹ n'en faisait pas davantage état. La

cyberstratégie américaine de 2018,¹⁰ également publiée par le Département de la Défense, n'utilise pas davantage la notion d'intelligence artificielle (ni celles associées).

Comme nous l'avons déjà mentionné, l'IA fait l'objet depuis peu (2019) aux Etats-Unis d'une doctrine officielle dans le domaine militaire. Mais ce document n'établit guère davantage de relation forte, particulière, entre IA et cyberspace. Ce dernier n'y est mentionné qu'à 4 reprises et précise uniquement que :

- La cybersécurité devra contribuer à sécuriser l'IA. la cybersécurité des plates-formes logicielles est une condition préalable au fonctionnement sûr des applications de l'IA. A cette fin des efforts particuliers seront faits pour développer des moyens de cybersécurité défensifs;
- L'IA sera un outil de sécurité, en améliorant la capacité de prédiction, d'identification et de réaction aux cybermenaces et aux menaces physiques.

Le directeur du JAIC (Joint Artificial Intelligence Center) évoquait en février 2019 son projet de travail commun avec le Cyber Commandement, la coopération pouvant porter sur la détection d'incidents et la cartographie de réseaux par exemple.

L'apport de l'IA à la dimension offensive est absente de ces considérations. Or nous savons que l'IA peut être intégrée dans des « cyber-armes » intelligentes, telles que des malwares dotés d'IA. L'IA dans le cyberconflit conserve les deux dimensions traditionnelles: défensive et offensive. Pour les penser, il est pratique de s'appuyer sur les connaissances acquises au cours des dernières décennies dans l'exploitation du cyberspace, et dans sa conceptualisation. Un travail important reste encore à faire pour intégrer pleinement l'IA dans les doctrines de cyberdéfense et comprendre par exemple comment ces technologies vont impacter chacune des trois couches du cyberspace (physique, logicielle et psycho-cognitive), pour appréhender et définir la fonction de « cyber-armes » autonomes, et penser enfin la nature de ces rapports de forces entre des belligérants qui pourront être pour les uns dotés de moyens de cyberdéfense augmentés par l'IA, pour les autres de moyens non augmentés par l'IA. L'IA sera-t-elle l'assurance d'une victoire sur des adversaires qui n'en disposeraient pas? La confrontation sera probablement plus complexe, car il n'est pas exclu que des stratégies puissent contrer la supériorité *a priori* de l'IA (nous savons cette dernière vulnérable à des leurre par exemple) d'une part; d'autre part, les IA ne sont ni ne seront toutes de qualité égale. On peut donc imaginer qu'une hiérarchie se crée entre IA, et ce tant dans le domaine « cyber » que dans les autres champs d'application.

7 <https://blog.marketresearch.com/8-key-military-applications-for-artificial-intelligence-in-2018>

8 Joint Chiefs of Staff, Cyberspace Operations, Joint Publication 3-12, 8 June 2018, 104 pages, Department of Defense, Washington DC., USA, https://www.jcs.mil/Portals/36/Documents/Doctrine/pubs/jp3_12.pdf?ver=2018-06-19-092120-930

9 Joint Chiefs of Staff, Cyberspace Operations, Joint Publication 3-12

(R), 5 February 2013, 70 pages, Department of Defense, Washington DC., USA, https://fas.org/irp/doddir/dod/jp3_12r.pdf

10 Department of Defense, Summary of the Cyber Strategy 2018, Septembre 2018, 10 pages, Washington DC., USA, https://media.defense.gov/2018/Sep/18/2002041658/-1/-1/1/CYBER_STRATEGY_SUMMARY_FINAL.PDF



De nombreux systèmes télé-opérés sont en passe de recevoir des composants IA afin de permettre la réduction du nombre d'opérateurs et ainsi, à gagner en autonomie.

Conclusion

L'intelligence artificielle aurait très bien pu relever des attributions des cyber-commandements ou d'agences comme la NSA, car elle est après tout fondamentalement « cyber ». Mais elle est au contraire traitée à part, comme un nouveau champ qui va imposer sa présence progressivement dans tous les espaces traditionnels (terre, air, mer, espace, et désormais cyberspace). Plutôt que d'IA, de manière générique, devrions-nous parler « des IA », désignant les multiples applications spécifiques au travers desquelles elle pourra déployer tout son potentiel.

L'engouement planétaire pour l'IA semble en faire l'un des enjeux majeurs et incontournables de ce début du 21^e siècle. Mais peut-être pourrait-on malgré tout envisager la possibilité d'un retournement de tendance. Qu'advierait-il de l'IA si une nouvelle fois elle décevait tous les espoirs placés en elle ?

D. V.

News

Nominations d'officiers généraux

Lors de sa séance du 19 août 2020, le Conseil fédéral a procédé aux nominations suivantes d'officiers généraux, avec effet au 1^{er} janvier 2021 et au 1^{er} juillet 2021.

Le commandant de corps Aldo C. Schellenberg, chef du commandement des Opérations et suppléant du chef de l'Armée, a fait valoir son droit à la retraite ordinaire et il sort du corps des instructeurs au 31 décembre 2020. Le Conseil fédéral le remercie pour les services rendus.

C'est le brigadier **Laurent Michaud** qui lui succédera au 1^{er} janvier 2021 en qualité de chef des Opérations ; le Conseil fédéral l'avait nommé à cette fonction lors de sa séance du 23 octobre 2019. La fonction de suppléant du chef de l'Armée sera pourvue à une date ultérieure.

Le brigadier **Peter Baumgartner**, actuel commandant de l'Ecole centrale reprend le commandement de la formation d'application de l'infanterie au 1^{er} janvier 2021.

Après sa formation d'agriculteur, Peter Baumgartner, 54 ans, a travaillé dans diverses entreprises agricoles avant de suivre une formation technico-commerciale. Conjointement à ses activités professionnelles, il a suivi des cours afin d'obtenir une maturité professionnelle de type D. En 1990, il a rejoint le Corps des instructeurs de l'infanterie et a depuis été engagé dans diverses fonctions au sein de l'armée. En 2003 et 2004, Peter Baumgartner a suivi le stage de formation pour les « Admiralstabs- und Generalstabsdienste » et le stage EURO auprès de la « Führungsakademie » de la Bundeswehr à Hambourg. En 2014, il a obtenu le *Master of Advanced Studies in Security Policy and Crisis Management* à l'EPFZ. Commandant de la brigade d'infanterie de montagne 12 de 2016 à 2017, Peter Baumgartner a été nommé commandant de l'Ecole centrale au 1^{er} janvier 2017 par le Conseil fédéral, avec promotion simultanée au grade de brigadier.

Le brigadier **Franz Nager**, actuel commandant de la formation d'application de l'infanterie devient commandant de l'Ecole centrale au 1^{er} janvier 2021.

Au bénéfice d'un brevet d'enseignement primaire, Franz Nager, 58 ans, est entré dans le corps des instructeurs de l'infanterie en 1991 et il a depuis été engagé dans diverses fonctions au sein de l'armée. En 2001, il a suivi l'« Infantry Captains Career Course » à Fort Benning, USA. En 2007, Franz Nager a en outre obtenu en 2007 le *Master of Advanced Studies in Security Policy and Crisis Management* à l'EPFZ. Le 1^{er} janvier 2012, le Conseil fédéral l'a promu au grade de brigadier et nommé au poste de commandant de la brigade d'infanterie de montagne 12. Le brigadier Franz Nager commande la formation d'application de l'infanterie depuis le 1^{er} juillet 2016.

Le colonel EMG **Peter Merz**, actuel chef de projet Nouvel avion de combat des Forces aériennes est nommé commandant des Forces aériennes au 1^{er} juillet 2021, avec promotion simultanée au grade de divisionnaire. Il succède au divisionnaire Bernhard Müller qui prend sa retraite anticipée le 30 juin 2021, avec remerciements pour les services rendus. Au bénéfice d'un CFC de mécanicien sur camions obtenu dans un lycée professionnel, Peter Merz, 52 ans, est entré à l'Escadre de surveillance des Forces aériennes en 1990 en tant que pilote militaire de carrière. Parallèlement à ses activités professionnelles, il a fréquenté l'école technique supérieure et obtenu le diplôme fédéral d'ingénieur HES. Peter Merz, a été engagé comme pilote militaire et moniteur de vol ainsi que dans diverses fonctions au sein de l'armée. Depuis le 1^{er} janvier 2018, il est en charge du projet Prochain avion de combat des Forces aériennes.

Source : Communication DDPS, 19.08.2020