Études de l'Ifri

Focus stratégique 84

INTELLIGENCE ARTIFICIELLE : VERS UNE NOUVELLE RÉVOLUTION MILITAIRE ?

Jean-Christophe NOËL

Octobre 2018

ifri Laboratoire de recherche sur la défense

L'Ifri est, en France, le principal centre indépendant de recherche, d'information et de débat sur les grandes questions internationales. Créé en 1979 par Thierry de Montbrial, l'Ifri est une association reconnue d'utilité publique (loi de 1901). Il n'est soumis à aucune tutelle administrative, définit librement ses activités et publie régulièrement ses travaux.

L'Ifri associe, au travers de ses études et de ses débats, dans une démarche interdisciplinaire, décideurs politiques et experts à l'échelle internationale.

Les opinions exprimées dans ce texte n'engagent que la responsabilité de l'auteur.

ISBN : 978-2-36567-922-0
© Tous droits réservés, Ifri, 2018

Comment citer cette publication :
Jean-Christophe Noël, « Intelligence artificielle : vers une nouvelle révolution militaire ? », *Focus stratégique*, n° 84, Ifri, octobre 2018.

Ifri

27 rue de la Procession 75740 Paris Cedex 15 – FRANCE

Tél. : +33 (0)1 40 61 60 00 – Fax : +33 (0)1 40 61 60 60

E-mail : accueil@ifri.org

Site internet : Ifri.org

Focus stratégique

Les questions de sécurité exigent une approche intégrée, qui prenne en compte à la fois les aspects régionaux et globaux, les dynamiques technologiques et militaires mais aussi médiatiques et humaines, ou encore la dimension nouvelle acquise par le terrorisme ou la stabilisation post-conflit. Dans cette perspective, le Centre des études de sécurité se propose, par la collection ***Focus stratégique***, d'éclairer par des perspectives renouvelées toutes les problématiques actuelles de la sécurité.

Associant les chercheurs du centre des études de sécurité de l'Ifri et des experts extérieurs, ***Focus stratégique*** fait alterner travaux généralistes et analyses plus spécialisées, réalisées en particulier par l'équipe du Laboratoire de Recherche sur la Défense (LRD).

Auteur

Jean-Christophe Noël est un ancien officier de l'armée de l'Air. Après avoir mené une carrière de pilote de chasse, il a tenu diverses places en état-major, traitant notamment des affaires de doctrine ou de prospective. Il a également été l'adjoint du chef de cabinet du chef d'état-major de l'armée de l'Air de 2006 à 2009, *Military Fellow* au Center for Strategic and International Studies à Washington D. C. en 2009 et expert chargé des affaires politico-militaires pendant cinq ans au Centre d'analyse, de prévision et de stratégie (CAPS) du Ministère des Affaires étrangères de 2012 à 2017. Il est actuellement chercheur associé à l'Ifri.

Comité de rédaction

Rédacteur en chef : Élie Tenenbaum

Assistante d'édition : Marie-Émilie Hennequart

Résumé

L'intelligence artificielle (IA) est un enjeu de défense prioritaire pour les puissances militaires du XXIe siècle. Sans surprise, les États-Unis et la Chine sont aujourd'hui en tête de cette nouvelle course aux armements digitalisée. En reproduisant les processus cognitifs au moyen d'algorithmes et de traitement automatisé du *big data*, l'IA est désormais capable d'effectuer un nombre grandissant de tâches spécifiques dans lesquelles elle surpasse les performances humaines. Appliquée au domaine militaire, elle permet de gérer et simuler l'environnement opérationnel, de détecter des menaces, de traiter et simplifier les masses de renseignement collectées et d'en livrer une analyse élémentaire. À ce titre, elle prolonge la révolution dans les affaires militaires survenue dans les années 1990 et se présente comme la voie principale de la supériorité tactique. Alors que l'automatisation s'affirme progressivement comme une nouvelle norme stratégique, les tenants d'un « humanisme militaire » soulignent cependant les limites de la technologie, le large éventail de contre-mesures et les risques d'une perte de contrôle, de déshumanisation de la guerre allant jusqu'à une remise en cause substantielle du métier de soldat. Si ces développements imposent de trouver à brève échéance un nouvel équilibre dans la relation homme-machine, l'avènement à plus long terme d'une IA dite « forte », entièrement autonome, pourrait transformer plus encore les dynamiques politico-militaires, voire altérer la nature même de la guerre.

Abstract

Artificial Intelligence (AI) is a priority defense issue for the military powers of the 21st century. Unsurprisingly, the United States and China are currently at the forefront of this new digitalized arms race. As AI aims to emulate cognitive processes with algorithms and automated processing of big data, it is capable to undertake a growing number of specific tasks in which it surpasses human performances. In the military field, it enables a better management and simulation of the operational environment, provide threats detection, process and simplify large quantities of collected intelligence and to deliver an elementary analysis. In this light, military AI perpetuates the Revolution in Military Affairs that began in the 1990s and now appears as the main path to achieving tactical superiority. As autonomy is progressively becoming a new strategic staple, proponents of a "military humanism" underline the limits of technology, the wide span of potential counter-measures as well as the risk of a loss of control, or a dehumanization of war leading to reconsider the warrior ethos. If these evolutions prompt for a new balance in man-machine teaming, the longer term prospect of the advent of a "strong AI", one that would be truly autonomous, could transform even more the political-military relationship, and even alter the very nature of the war.

Sommaire

INTRODUCTION 11

Un enjeu de défense 12

Définir l'intelligence artificielle 14

QU'EST-CE QUE L'INTELLIGENCE ARTIFICIELLE ? 17

Une brève histoire de l'intelligence artificielle 17

Comment cela fonctionne-t-il ? 20

Quelques applications civiles 21

L'INTELLIGENCE ARTIFICIELLE ET L'ART DE LA GUERRE 25

Des premières tentatives décevantes 25

Les applications militaires à court terme 27

Gérer et simuler l'environnement 28

Détecter et traiter 28

Simplifier 30

Automatiser 31

Prédire 31

La poursuite de la Révolution dans les affaires militaires 32

Quelle influence sur la préparation des forces et les opérations ? 35

Améliorer l'entraînement, la simulation et la conception des équipements 35

Accélération du rythme des opérations 36

Vers l'hyperpersonnalisation de la guerre ? 39

UNE RELATION HOMME-MACHINE TRANSFORMÉE 43

Vers l'automatisation comme norme ? 43

Quand l'homme domine la machine : l'apport de l'humanisme militaire 46

Les limites technologiques 46

La perte de contrôle 48

Des contre-stratégies efficaces 50

L'humanisme militaire 53
L'équipier fidèle 55
Une troisième voie : regrouper les robots en troupeau **56**
Contrôler sans dominer 56
L'ère des centaures 58
Les robots domestiqués 59
Vers une utilisation sociale de l'intelligence artificielle 60
Confident ou commissaire politique ? 62
EN ROUTE VERS UNE INTELLIGENCE ARTIFICIELLE FORTE **65**
Miser sur l'intelligence artificielle **65**
Le pari chinois : un projet structurant 65
Les « hivers » de l'intelligence artificielle 67
Une technologie nouvelle pour faire face à des problèmes classiques .. 67
Culture politique, doctrine militaire et intelligence artificielle **69**
Intelligence artificielle forte et transformation de la guerre **71**
De l'anticipation à la guerre préventive 71
Les affrontements entre IA 73
Vers un changement de nature de la guerre ? 74
CONCLUSION **77**

Introduction

L'intelligence artificielle (IA) est un terme indiscutablement à la mode. Elle incarne avec justesse le phénomène de disruption, qui pointe une accélération inéluctable du cycle de l'innovation technologique et annonce un bouleversement durable des activités humaines[1]. Le nombre d'applications pratiques de l'intelligence artificielle dans la vie quotidienne se multiplie et suscite un changement visible, et parfois inattendu, des comportements[2]. Malgré les espoirs suscités par ces progrès, de nombreux scientifiques ou experts sont très alarmistes. Le physicien Stephen Hawkins craignait que l'IA, « en se redéfinissant de plus en plus vite » de manière autonome, évolue bien plus rapidement que l'homme et finisse par le dépasser[3]. Le futurologue américain Ray Kurzweil estimait quant à lui que « le point de singularité », qui marque le moment où l'intelligence des machines dépasserait celle des hommes et pourrait décider de leur destin, adviendrait en 2030[4].

Dans son best-seller *Homo Deus : une brève histoire de l'avenir*[5], l'auteur israélien Yuval Noah Harari affine le raisonnement. Il présente un scénario où le monde est divisé entre des hommes augmentés, formant une élite qui s'appuie sur des ordinateurs très évolués pour traiter toujours plus de données et améliorer sans cesse leurs connaissances, et des hommes ordinaires, composant la majorité de l'humanité, devenus inutiles car dépassés par des machines accomplissant bien mieux leurs tâches. Tous ces hommes sans but ne tiennent plus aucune fonction économique ou sociale. Ils végètent dans un monde qui n'est plus fait pour eux.

---

1. Sur la disruption, voir par exemple J.-M. Dru, *New : 15 approches disruptives de l'innovation*, Londres, Pearson Education, 2016 ; B. Stiegler, *Dans la disruption : comment ne pas devenir fou ?*, Paris, Les liens qui libèrent, 2016 ; P. Perrineau, *Le vote disruptif*, Paris, Presses de Sciences-Po, 2017 ; S. Claeys, *De disruption à prosommateur : 40 mots-clés pour le monde de demain*, Paris, Le Pommier, 2018 ; S. Mallard, *Disruption – Intelligence artificielle, fin du salariat, humanité augmentée*, Paris, Dunod, 2018.

2. Il est désormais possible de lâcher le volant et de laisser sa voiture effectuer toute seule un créneau ou de parler à son téléphone portable, son téléviseur ou un assistant vocal robotisé, comme s'il était un être humain, pour chercher un renseignement.

3. S. Hawking, « AI Could Spell End of the Human Race », *BBC News*, 2 décembre 2014.

4. R. Kurzweil, *The Singularity is Near: When Human Transcends Biology*, New York, Viking Press, 2005.

5. Y. N. Harari, *Homo Deus : une brève histoire de l'avenir*, Paris, Albin Michel, 2017.

Le développement de l'intelligence artificielle peut donc défaire l'ensemble des valeurs qui nous gouvernent et mener à l'extinction d'*homo sapiens*. Cette vision dystopique appelle deux remarques. La première est qu'elle renvoie à un réflexe classique, qui voudrait qu'en imitant Dieu, l'homme transgresse l'ordre des choses. Il devra naturellement en assumer le coût, comme ont dû le faire le rabbin de Prague Loew, accablé par les exactions du Golem, ou le docteur Frankenstein, traquant désespérément le monstre hideux et meurtrier qu'il avait créé avant de l'abandonner[6]. Le sujet de l'intelligence artificielle est très chargé symboliquement.

La seconde remarque est très largement inspirée du livre *Le mythe de la singularité* du philosophe français Jean-Gabriel Ganascia, qui s'interroge sur la prégnance du discours associant intelligence artificielle et disparition de l'humanité[7]. Il considère notamment que cette thèse est privilégiée par certains acteurs privés et médiatiques pour évacuer les débats sociétaux essentiels et poursuivre le développement d'applications commerciales souvent fructueuses en gains financiers. Il semble en effet aujourd'hui essentiel d'envisager avec plus d'objectivité les conséquences du développement de l'intelligence artificielle à court et moyen terme sur la vie de la Cité. Il sera alors plus aisé de débattre sereinement des évolutions possibles et de les accompagner dans un sens bénéfique.

Un enjeu de défense

Parmi les débats les plus médiatiques autour de l'intelligence artificielle, celui sur la défense paraît capital dans ce nouveau contexte. Il consiste à se demander comment l'intelligence artificielle va être utilisée dans le domaine militaire et comment elle pourrait influencer l'art de la guerre. La question de la distribution de la puissance militaire et des ressources qu'elle offre est en jeu. Les plus grandes nations militaires s'emparent toutes de ce débat et ont choisi d'investir dans le développement de l'IA. Le sous-secrétaire à la Défense américain, Robert Work, a par exemple soutenu la *Third Offset Strategy* – ou Troisième stratégie de compensation – pour donner les moyens aux forces américaines de continuer à s'imposer décisivement dans les guerres conventionnelles[8].

6. G. Meyrink, *Le Golem*, Paris, Flammarion, 2003 ; M. Shelley, *Frankenstein ou le Prométhée moderne*, Paris, Folio, 2015.
7. G. Ganascia, *Le mythe de la singularité. Faut-il craindre l'intelligence artificielle ?*, Paris, Seuil, 2017.
8. « We believe quite strongly that the technological sauce of the Third Offset is going to be advances in Artificial Intelligence (AI) and autonomy » cité *in* B. Work, « Remarks by Deputy Secretary Work on Third Offset Strategy », U.S. Department of Defense, Bruxelles, 28 avril 2016 ; disponible sur : defense.gov.

Pékin s'est également mis en ordre de bataille. Le Conseil d'État chinois a publié en juillet 2017 le *Plan de développement de la nouvelle génération de l'intelligence artificielle* dans lequel l'IA est présentée comme un « nouveau point focal de la compétition internationale ». Il est même ajouté qu'elle sera « une technologie stratégique qui commandera le futur ». Le but clairement énoncé par la Chine est de devenir le premier centre d'innovation pour l'IA dans les années 2030 et d'être la puissance la plus avancée dans ce domaine[9]. Vladimir Poutine a pour sa part déclaré le 1er septembre 2017 que cette technologie recelait « des possibilités colossales et des menaces difficilement envisageables ». Il ajoutait même que « celui qui deviendrait le leader dans ce domaine sera le maître du monde[10] ». En France, la classe politique s'est officiellement emparée de cette problématique au même moment. Le 14 février 2017, Jean-Yves Le Drian, alors ministre de la Défense, affirmait que « l'intelligence artificielle est un élément de [notre] souveraineté nationale[11] ».

Plus récemment, le 16 mars 2018, la ministre des Armées Florence Parly était présente lors du lancement de l'étude *Man Machine Teaming* (MMT), conduite par Dassault Aviation, dont le but est d'explorer le potentiel de l'intelligence artificielle pour l'aviation de combat. Elle dévoila à cette occasion un plan pour promouvoir le développement de l'IA dans les armées, avec notamment un investissement progressif de 100 millions d'euros par an et le recrutement d'une cinquantaine d'experts supplémentaires en matière de *Data Science* et d'intelligence artificielle[12]. Enfin, le rapport Villani, intitulé *Donner un sens à l'intelligence artificielle : pour une stratégie nationale et européenne*[13], a identifié la défense comme l'un des quatre secteurs stratégiques dans lesquels la France et l'Europe doivent investir s'ils souhaitent tenir leur rang dans la compétition internationale qui se profile.

En attendant que les robots et les ordinateurs animés par une superintelligence ne nous asservissent ou nous remplacent un jour, l'intelligence artificielle présente un enjeu reconnu au plus haut niveau dans le domaine de la défense, en ce qu'elle paraît avoir le potentiel d'offrir la supériorité militaire à ceux qui sauront le mieux maîtriser son développement.

9. En chinois, disponible sur : www.gov.cn.
10. « Pour Vladimir Poutine, le pays leader en matière d'intelligence artificielle sera "maître du monde" », *RT France*, 1er septembre 2017, disponible sur : francais.rt.com.
11. J.-Y. Le Drian, Colloque « Intelligence artificielle : des libertés individuelles à la sécurité nationale », Paris, Assemblée nationale, 14 février 2017.
12. « Florence Parly présente son plan en faveur de l'intelligence artificielle », Ministère des Armées, 19 mars 2018, disponible sur : www.defense.gouv.fr.
13. C. Villani, « Donner un sens à l'intelligence artificielle : pour une stratégie nationale et européenne », Rapport remis au Premier ministre, mars 2018.

Définir l'intelligence artificielle

Si l'engouement pour l'intelligence artificielle est partagé par de nombreux responsables politiques, il est plus difficile de trouver une définition commune à laquelle adhéreraient sans réserve les experts de la discipline. La question est loin d'être simple alors que la description même de l'intelligence humaine devient de plus en plus complexe[14] et sa caractérisation de plus en plus débattue. Plusieurs types de définition cohabitent néanmoins aujourd'hui, qui possèdent chacune leur intérêt.

Le chercheur en informatique français, directeur des études chez Facebook et titulaire de la « chaire intelligence artificielle » au Collège de France, Yann LeCun estime par exemple que l'IA doit permettre de « faire faire aux machines des activités qu'on attribue généralement aux animaux et aux humains[15] ». Cette définition très synthétique a le mérite de caractériser simplement l'objectif des chercheurs. Le comportement des êtres humains et leurs réalisations sont posés en référence, en mètre étalon. L'effet pervers d'une telle approche est peut-être de donner l'impression qu'IA et individu sont interchangeables, ce qui peut déranger à l'heure où l'IA est dénoncée comme un rival potentiel de l'homme plutôt que comme un outil complémentaire.

Cédric Villani complète cette définition en indiquant que l'intelligence artificielle est d'abord une quête, « un programme fondé autour d'un objectif ambitieux : comprendre comment fonctionne la cognition humaine et la reproduire ; créer des processus cognitifs comparables à ceux de l'être humain[16] ». Cette définition apporte un élément dynamique en rappelant que l'intelligence artificielle est d'abord un projet, une ambition. Penser l'intelligence artificielle nécessite de faire constamment la différence entre ce qui est et ce qui sera peut-être.

Ainsi, Mary L. Cummings, ancienne pilote de chasse de l'*US Navy* et actuellement directrice du *Humans and Autonomy Laboratory* à Duke University, définit l'IA comme « la capacité d'un système informatique à accomplir des tâches qui nécessitent normalement de l'intelligence humaine, telle que la perception visuelle, la reconnaissance des paroles et la prise de décision[17] ». Les exemples cités sont précis, mais ne renvoient pas à des tâches démesurées. La prise de décision n'a pas nécessairement

14. H. Gardner, *Les formes de l'intelligence*, Paris, Odile Jacob, 1997.
15. *Comment l'Intelligence Artificielle va changer vos vies*, Paris, Libération/France Inter, décembre 2017, p. 11.
16. C. Villani, « Donner un sens à l'intelligence artificielle : pour une stratégie nationale et européenne », *op. cit.*, p. 9.
17. M. L. Cummings, *Artificial Intelligence and the Future of Warfare*, Chatham House, janvier 2017, p. 2.

lieu dans un environnement complexe. C'est d'ailleurs le thème qu'elle développe en qualifiant d'« épineux[18] » le chemin qui reste devant les chercheurs.

En s'inspirant largement des propositions qui viennent d'être évoquées, l'intelligence artificielle sera considérée dans ce document comme un ensemble de techniques visant à configurer la matière pour qu'elle réponde efficacement à des tâches cognitives, selon des procédés qui ne sont pas nécessairement déduits de l'expérience humaine. Si son intérêt est limité aujourd'hui à des tâches spécifiques et limitées (IA dite « faible »), l'objectif est de se rapprocher (IA dite « forte »), ou même de dépasser (superintelligence) les performances cognitives des êtres humains sur l'ensemble des fonctions qu'ils accomplissent.

Dans ce cadre, cette étude a pour ambition de réfléchir à la manière dont l'intelligence artificielle pourrait justement influencer un domaine particulier de l'activité humaine, à savoir la guerre et la stratégie. Pour répondre à cette question, il s'agira d'abord d'appréhender les contours de l'intelligence artificielle et de présenter ses applications actuelles dans le domaine civil (1). Sur le plan militaire ces applications s'insèrent dans un vaste mouvement amorcé avec la Révolution dans les affaires militaires des années 1990 qui participe à l'accélération du rythme des opérations tout en suscitant une hyperpersonnalisation de la guerre (2). Il s'agira ensuite de s'intéresser à la manière dont l'intelligence artificielle peut modifier d'un point de vue militaire les relations entre les hommes et les machines, mais aussi entre les hommes entre eux. Si les choix dépendront *in fine* de la fiabilité de l'intelligence artificielle, l'importance des aspects culturels devra aussi être prise en compte(3). Enfin, la dernière partie mettra en lumière plusieurs débats qui ne seront tranchés que lorsque l'usage de l'intelligence artificielle sera répandu dans les armées, comme le fait de savoir si l'IA peut un jour transformer la nature de la guerre (4).

18. *Ibid*., p. 12.

Qu'est-ce que l'intelligence artificielle ?

Une brève histoire de l'intelligence artificielle

Alan Turing est souvent considéré comme le premier savant de l'époque contemporaine à avoir initié la réflexion sur le thème de l'intelligence et des ordinateurs[19]. Il commence l'un de ces plus fameux articles, « *Computing Machinery and Intelligence* », écrit en 1950, par la question suivante : « Est-ce que les machines peuvent penser ?[20] ». Il estime que cette éventualité est plausible et répond à une liste d'objections. Il faut néanmoins attendre quelques années encore pour que l'intelligence artificielle émerge comme un domaine de recherche scientifique autonome. Une dizaine de chercheurs se réunissent pendant l'été 1956 pour assister à un séminaire consacré à ce thème au Dartmouth College dans le New Hampshire. John McCarthy, l'un de ses organisateurs, introduit pour la première fois le terme d'« intelligence artificielle » dans le document de présentation. L'objectif est alors de se distinguer à la fois des études très en vogue sur les automates, dont il estime que la théorie reste limitée, et des recherches sur la cybernétique, dominées à l'époque par le mathématicien Norbert Wiener qui règne sur la discipline[21]. McCarthy précise que « l'enjeu est d'élaborer une machine qui se comporte d'une manière qu'on qualifierait d'intelligente si un être humain se comportait de la sorte[22] ».

Les travaux sont fructueux et bientôt, les premières applications apparaissent. Arthur Samuel développe par exemple dans les années 1950 un programme s'appuyant sur l'apprentissage automatique, capable de battre de bons joueurs au jeu de dames. Les premiers « chatbots[23] » sont construits dans les années 1960 : ELIZA, l'un d'entre eux, simule la présence d'un psychologue. Le programme peut poser automatiquement certaines questions quand les propos d'un patient contiennent des mots-clés comme « mère » ou « père ». Il est en revanche incapable de répondre aux questions ouvertes.

---

19. Pour une histoire de l'IA jusqu'à 2009, lire : N. J. Nilsson, *The Quest for Artificial Intelligence: A History of Ideas and Achievements*, Cambridge, Cambridge University Press, 2009.
20. A. M. Turing, *Computing Machinery and Intelligence,* Oxford, Mind, 1950, p. 433-460, disponible sur : www.csee.umbc.edu.
21. *Ibid*., p. 78.
22. N. J. Nilsson, *The Quest for Artificial Intelligence, op. cit*., p. 77.
23. Logiciel programmé pour simuler une conversation naturelle.

Deux écoles de pensée émergent alors : les connexionnistes et les symbolistes. Les premiers proposent de s'inspirer de la nature afin de simuler par ordinateur la manière dont fonctionne le cerveau humain, copiant ainsi de manière très simpliste, les réseaux de neurones. Les seconds préfèrent s'en tenir aux prédicats logiques pour arriver à leurs fins. Ils s'appuient notamment sur les « systèmes experts », qui dominent les premiers développements de l'intelligence artificielle. Le raisonnement à suivre pour résoudre un problème est décortiqué, codifié et transformé en une succession d'actions logiques relativement simples que la machine effectue très rapidement. Une recommandation finale est proposée à l'opérateur, qui est censé la suivre.

La discipline connaît un premier « hiver » à partir des années 1970 avec un net ralentissement de l'intérêt général pour cette technologie et une baisse sensible des dépenses publiques. Certaines promesses ambitieuses ne sont pas tenues et engendrent une déception légitime. Marvin Minsky, qui dirige alors le Laboratoire d'intelligence artificielle du Massachussetts Institute of Technology (MIT), déclarait par exemple en 1968 après la sortie du film de Stanley Kubrik *2001, l'Odyssée de l'espace* que « d'ici 30 ans, nous devrions avoir des machines dont l'intelligence est comparable à celle de l'homme[24] ». Mais la technologie fait défaut à la théorie. Comme le fait remarquer le roboticien Hans Moravec, l'intelligence artificielle a besoin d'ordinateurs puissants pour fonctionner, comme les avions ont besoin de réacteurs avec une grande poussée pour décoller. Or, les performances des ordinateurs des années 1970 sont encore insuffisantes[25]. Par ailleurs, des problèmes qui semblent simples à accomplir pour l'homme sont difficiles à réaliser par un ordinateur ou un robot. Marcher sur un sol irrégulier s'avère par exemple très compliqué[26]. Enthousiasmés par leurs premiers résultats, des chercheurs ont péché par excès d'optimisme.

L'engouement revient au début des années 1980 avec le développement de nouveaux langages informatiques, comme Prolog ou LISP, et de systèmes experts plus élaborés. Les Japonais comme les Britanniques dépensent environ 850 millions de dollars pour mettre au point des ordinateurs à la pointe de la performance. La *Defense Agency Research Projects Agency* (DARPA), agence de recherche et développement américaine des technologies militaires, multiplie les programmes. Mais la déception est encore une fois au bout de la route.

24. N. J. Nilsson, *The Quest for Artificial Intelligence, op. cit.*, p. 163.
25. H. Moravec, *The Role of Raw Power in Intelligence*, Stanford, Stanford Libraries, 12 mai 1976, disponible sur : www.frc.ri.cmu.edu.
26. Ce constat est appelé aujourd'hui « paradoxe de Moravec ».

L'intelligence artificielle connaît un second hiver de la fin des années 1980 au début des années 1990. Les outils et les langages des superordinateurs sont dépassés par de nouveaux venus : les ordinateurs « personnels » développés par Apple ou IBM évoluent très rapidement et s'avèrent être les plus puissants et les plus performants. Par ailleurs, les règles des systèmes experts sont fastidieuses à concevoir et trop lourdes à mettre à jour. Elles ne sont efficaces que dans certains contextes et ne peuvent évoluer par elles-mêmes. La recherche semble encore être dans une impasse.

L'espoir point une nouvelle fois avec les années 1990, mais les progrès sont lents. Des épisodes fameux servent la cause de l'intelligence artificielle, comme la victoire du programme *Deep Blue* en 1997 contre le champion du monde des échecs Garry Kasparov. Le logiciel calcule alors 200 000 millions de positions par seconde[27]. Il teste toutes les possibilités pour résoudre le problème sur l'échiquier et choisit le chemin le plus performant. Le principe de « force brute » triomphe dans ce cadre précis et offre une revanche aux symbolistes. D'autres voies sont cependant explorées dans une direction plus connexionniste. C'est par exemple le cas de la reconnaissance de caractères. Des logiciels peuvent désormais analyser des écrits, des nombres et mettre à profit les données rassemblées dans une application pratique, par exemple pour lire électroniquement des chèques à encaisser.

C'est finalement au tournant des années 2010 que les percées technologiques les plus décisives se concrétisent. Le contexte informatique a évolué et trois facteurs principaux permettent de soutenir ces progrès. Les algorithmes progressent en qualité et les réseaux de neurones peuvent être associés entre eux, formant plusieurs « couches ». En outre, la puissance de calcul des ordinateurs augmente sans cesse à prix constant. La loi imaginée en 1965 par Gordon Moore, cofondateur de la société Intel, continue d'être vérifiée jusqu'en 2016, avec le doublement de la puissance de calcul des processeurs tous les dix-huit mois – même si un certain ralentissement semble se dessiner sur la fin[28]. Enfin, le nombre de données disponibles pour entraîner les ordinateurs explose littéralement. Jean-Gabriel Ganascia souligne par exemple que le stockage des données échangées en 2015 sur Internet pourrait remplir l'équivalent de 500 000 millions de Bibliothèque nationale de France[29]. Sans *big data*, l'intelligence artificielle ne peut tout simplement pas fonctionner.

27. O. Ezratty, *Les usages de l'intelligence artificielle*, 17 novembre 2017, p. 26, disponible sur : www.oezratty.net.
28. M. Mitchell Waldrop, « The Chips Are Down for Moore's Law », *Nature*, 9 février 2016, disponible sur : www.nature.com.
29. J. G. Ganascia, *Le mythe de la singularité, op. cit.*, p. 47.

Comment cela fonctionne-t-il ?

Les applications les plus médiatisées aujourd'hui sont celles qui sont dérivées des réseaux de neurones et de l'apprentissage machine (*machine learning*). Poursuivant les avancées connexionnistes en matière de reconnaissance de caractère, les technologies de l'identification connaissent un véritable essor. Le principe est d'entraîner une machine à reconnaître certaines caractéristiques d'un objet, au travers d'une image par exemple. Des opérateurs proposent au logiciel des millions d'images encodées en lui précisant si elles représentent ou non l'objet considéré. Très schématiquement, l'image est transformée en une série de nombres (ou vecteur caractéristique) par le logiciel qui indique la présence ou l'absence d'un motif simple de l'image. Cette série de nombres est pondérée par d'autres nombres (ou « poids ») pour obtenir un résultat final. Si le quotient est supérieur à un certain seuil, l'objet de l'image appartient à la classe voulue. Si le logiciel classe mal l'image de l'objet, les poids sont ajustés jusqu'à ce que l'image soit rangée dans la bonne catégorie type. À force d'itérations, la machine limite sa marge d'erreur. Elle est alors capable de catégoriser des images qu'elle n'avait même jamais vues.

L'apprentissage profond (*deep learning*) est une évolution de l'apprentissage machine, avec la constitution d'un réseau multi-couches d'éléments simples[30]. Les couches de neurones sont interconnectées entre elles. Chacune analyse l'ensemble de l'image au travers de dizaine de millions de calculs élémentaires, mais en se spécialisant. Les premières couches traitent des informations les plus simples (des pixels), les couches intermédiaires et finales définissent des concepts plus compliqués pour lesquelles elles ne sont pas entraînées initialement (comme les formes ou les traits d'un visage). Encore une fois, une bonne ou mauvaise classification finale entraîne le maintien ou la modification des paramètres internes de la machine. Les résultats sont affinés de manière autonome grâce à la méthode de rétro-propagation, qui ajuste les paramètres de chaque couche de chaque module. Tout se passe comme si la machine apprenait de ses erreurs et se perfectionnait en même temps qu'elle avait accès à des données supplémentaires[31].

30. L'apprentissage profond est évoqué dès les années 1980. Ce n'est donc pas une découverte théorique. Mais les conditions informatiques de son développement n'étaient pas présentes alors.
31. Le lecteur curieux et désireux d'approfondir ses connaissances pourra consulter le dossier de presse correspondant à la leçon suivante : Y. LeCun, « L'apprentissage profond : une révolution en intelligence artificielle », Collège de France, leçon inaugurale du 4 février 2016, disponible sur : www.college-de-france.fr.

Plusieurs types d'apprentissage existent. L'apprentissage supervisé est le plus répandu où l'homme fournit les données à la machine pour qu'elle apprenne. Elle acquiert progressivement de l'autonomie. L'apprentissage par renforcement utilise l'expérience que la machine acquiert pour optimiser une récompense. Des intelligences artificielles ont par exemple appris à jouer aux jeux vidéo. Constatant qu'elles obtiennent les meilleurs scores en privilégiant certains mouvements ou décisions, elles les retiennent et se perfectionnent de la sorte progressivement[32]. Enfin, l'apprentissage non supervisé, a pour but de laisser la machine apprendre seule par l'observation, sans que les classes des objets qu'on lui propose soient *a priori* définies. Elle doit être capable de faire apparaître à terme des catégories en fonction des propriétés récurrentes des données qu'elle reçoit. L'apprentissage profond fonctionne donc par induction. L'observation d'exemples permet la détection de régularité et leur extrapolation en des principes généraux.

Quelques applications civiles

En 2012, les algorithmes qui fonctionnent sur le principe de l'apprentissage machine sont adoubés lors du concours de reconnaissance d'images *ImageNet*. Ils obtiennent un taux d'erreur de seulement 16,4 %, valeur qui n'avait encore jamais été atteinte[33]. L'année suivante, tous les logiciels inscrits au concours fonctionnent selon la logique de l'apprentissage profond. Les applications se multiplient depuis et les logiciels sont désormais capables de reconnaître des sons, des paroles, des textes, des individus ou des objets dans des films, des lieux de vie ou dans la nature. La maîtrise de ces briques technologiques est essentielle pour envisager le développement des voitures autonomes, puisqu'elles devront reconnaître dans leur environnement les passants, les véhicules ou les panneaux de signalisation.

Les progrès sont également remarquables dans le domaine de la santé où les bases de données sont très bien alimentées. Une équipe internationale de chercheurs a ainsi annoncé le 29 mai 2018 que des logiciels avaient réussi à mieux détecter que des spécialistes des cancers de la peau sur une série de photos médicales. Ils parvenaient à identifier 95 % des mélanomes contre 87 % pour les médecins[34]. En utilisant les données déjà enregistrées chez d'autres patients, l'intelligence artificielle pourra

32. P. Scharre et M. C. Horowitz, « Artificial Intelligence: What Every Policymaker Needs to Know », *Center for a New American Security*, 2018, p. 5, disponible sur : www.cnas.org.
33. Il était proche de 25 % les années précédentes.
34. F. Méréo, « L'intelligence artificielle au secours de la lutte contre le cancer », *Le Parisien*, 1er juin 2018.

prédire avec une bonne probabilité la manière dont la maladie se développera en fonction de la forme de la tumeur et de l'état du patient, et peut-être proposer les remèdes les mieux adaptés.

Dans le domaine des jeux, l'intelligence artificielle *AlphaGo* de la société *DeepMind* est parvenue à battre en mars 2016 le meilleur joueur de Go mondial, le Coréen Lee Sedol. La performance est supérieure à celle de *Deep Blue* car les combinaisons dans le jeu de Go sont bien plus élevées qu'aux échecs, du fait d'une aire de jeu plus grande et de possibilités de positionnement moins contraints. *AlphaGo* s'est entraîné en étudiant plus de 150 000 parties jouées par les meilleurs spécialistes. Le programme exploitait à la fois les ressources des logiciels de force brute et d'apprentissage profond, ne testant ainsi que les coups les plus prometteurs[35]. Le triomphe d'*AlphaGo* n'a toutefois été que de courte durée car il est déjà dépassé par une version plus élaborée, appelé *AlphaGo Zero*, qui s'est entraînée contre elle-même en jouant 4,9 millions de parties. Elle s'est seulement mesurée après à *AlphaGo*, qu'elle a écrasé[36]. L'intervention de l'homme dans l'apprentissage de ce logiciel, capable de triompher dans une simulation abstraite de la guerre vieille de 2 500 ans, a été minimale[37].

Plus remarquable encore, l'intelligence artificielle l'emporte désormais dans des jeux où la situation d'informations est imparfaite, comme au poker. Lors d'une compétition de 20 jours à Pittsburgh où 120 000 mains furent jouées, le logiciel *Libratus* s'imposa en battant d'excellents joueurs[38]. *Libratus* ne suit pas une stratégie qui consisterait à deviner la conduite de l'adversaire humain en fonction des parties qu'il a déjà jouées car le joueur humain, conscient de la supériorité de la machine dans ce domaine, pourrait être tenté de modifier sensiblement son style de jeu. Les programmateurs cherchent plutôt à faire une analyse statistique du risque en fonction des deux cartes que possède la machine et à le pondérer en tenant compte de la valeur des jetons déjà engagés sur la table et des possibilités de relance de l'adversaire. Il s'agit alors moins de gagner chaque partie que de ne pas la perdre, ce qui s'avère être la meilleure

35. O. Ezratty, *Les usages de l'intelligence artificielle, art. cit.*, p. 27.
36. D. Silver, J. Schrittwieser, *et al.*, « Mastering the Game of Go Without Human Knowledge », *Nature*, vol. 550, 2017, disponible sur : www.nature.com.
37. C. B. Cain, « Go and Artificial Intelligence: Potential for Strategic Decision-Making », *Strategy Research Project*, US Army War College, 2017, p. 1, disponible sur : publications.armywarcollege.edu.
38. Les parties se sont déroulées selon les règles du *Head's-up, No Limit Texas Hold'em*. Dans cette version du poker, chaque joueur reçoit deux cartes dont il est le seul à connaître la valeur. Cinq cartes sont ensuite tirées et sont dévoilées devant l'ensemble des joueurs. Le vainqueur est celui qui affiche la meilleure combinaison entre ses cartes et celles qui sont découvertes. Les joueurs ont la possibilité de miser le nombre de jetons qu'ils veulent, mais ils doivent accepter de suivre la mise de leur adversaire pour rester en jeu.

option dans la durée. La machine peut ainsi s'imposer face à l'homme en dehors d'un cadre normatif strict, où quelques règles définissent les possibilités des uns et des autres. Elle peut vaincre en prenant en compte des données incomplètes ou dissimulées. En même temps, tout se passe comme si les algorithmes parvenaient déjà à appréhender en partie le hasard et la psychologie humaine[39].

Si l'histoire de l'intelligence artificielle est récente et s'est déroulée en dents de scie, cette technologie s'est néanmoins développée rapidement et conquiert régulièrement de nouveaux territoires en offrant des applications originales, quoiqu'encore limitées, où elle dépasse les performances cognitives de l'homme. Les ressources qu'elle offre peuvent évidemment être transposées dans le domaine militaire, dans le but d'améliorer les performances des armées. C'est l'objet d'étude de la prochaine partie, qui décrira également comment ces ressources favorisent certains types de stratégie.

39. N. Brown et T. Sandholm, « Superhuman, AI for Heads-Up No-Limit Poker: *Libratus* Beats Top Professionals », *Science*, vol. 359, 26 janvier 2018, p. 418-424, disponible sur : science.sciencemag.org ; A. Laurent, « Comment une intelligence artificielle ridiculise les meilleurs joueurs de poker », *Numerama*, 27 janvier 2017, disponible sur : www.numerama.com.

L’intelligence artificielle et l’art de la guerre

L’usage de l’intelligence artificielle, dans son acception actuelle, est récent dans les forces armées. Il est donc prématuré de tirer des leçons définitives de ces expériences. Le futur de l’intelligence artificielle militaire peut, au mieux, être esquissé. En revanche le traitement plus ou moins automatisé d’importantes autres masses de données est un domaine lié à l’IA qui possède déjà une longue histoire militaire[40]. Certains enseignements spécifiques peuvent donc en être tirés. En 1884, le professeur au MIT Herman Hollerith crée ainsi une machine qui trie des cartes perforées à des fins de sondages ou de recensements. Des machines de ce type sont employées pendant la Première Guerre mondiale pour procéder à l’évaluation psychologique des jeunes conscrits sur une large échelle. Lors de la Seconde Guerre mondiale, des tests psycho-sociaux sont entrepris sur les officiers et les conscrits et sont compilés afin de mieux connaître les caractéristiques des individus en guerre. Les résultats seront à l’origine d’un ouvrage de référence de la sociologie militaire, *The American Soldier*[41].

Des premières tentatives décevantes

Toutefois l’exploitation militaire la plus fameuse – et la plus controversée – des données de masse est probablement celle effectuée pendant la guerre du Vietnam sous l’impulsion du secrétaire à la Défense Robert McNamara. Ancien professeur d’économie à la Harvard Business School, ce dernier a appliqué avec succès une approche statistique du management au sein de l’entreprise Ford, ce qui lui vaut de prendre la tête de l’entreprise. Persuadé que la quantification contribue à une meilleure prise de décision, il charge Alain Enthoven, nommé Secrétaire assistant à l’analyse des systèmes, d’introduire ses méthodes de travail au Pentagone. Enthoven recrute de jeunes et brillants assistants, surnommés les *Whiz Kids*, pour animer un nouveau programme, le *Planning, Programming, Budgeting System* (PPBS). Ils s’appuient sur des données statistiques traitées par ordinateurs pour faire de la recherche opérationnelle, de l’aide à la prise de décision.

40. D. F. Harrison, « Computers, Electronic Data and the Vietnam War », *Archivaria*, vol. 26, été 1988, p. 18-32.
41. S. A. Stouffer, *The American Soldier*, Princeton, Princeton University Press, 1949.

Cette approche de la guerre bouleverse les habitudes et est violemment critiquée par certains militaires, notamment lorsqu'elle est appliquée au cours de la guerre du Vietnam[42]. Une histoire fameuse symbolise les limites de cette « approche informatique » qui fait la part belle aux mesures (*metrics*) en tout genre. En 1969, toutes les données connues sur le Vietnam et les États-Unis, comme la population, le produit national brut, les capacités de production ou la taille des armées, sont introduites dans un ordinateur. Un analyste américain demande alors à l'ordinateur « quand gagnerons-nous ? ». Après un bref instant, la machine lui répond : « vous avez gagné en 1964 ![43] »

Le décompte des pertes ennemies (ou *body count*) est probablement l'indicateur qui illustre le mieux la faillite de ce modèle. Ce marqueur devint une telle obsession, selon certains généraux comme Douglas Kinnard, que des soldats américains prennent des risques inutiles pour comptabiliser le nombre de Viêt-Cong morts et trouvent parfois la mort[44]. Le *body count* devient une fin en soi, qui égare des analystes incapables de lier les résultats tactiques et leurs effets opératifs et stratégiques. Les données envoyées vers les échelons les plus élevés sont par ailleurs volontairement souvent faussées pour satisfaire les attentes de la hiérarchie. Les indicateurs les plus convaincants ou significatifs, comme « les sourires que (des soldats) voyaient sur les visages des gens tandis qu'(ils) marchaient à travers les hameaux[45] », ne sont pas pris en compte ou sont impossibles à mesurer.

Cet échec condamne-t-il définitivement ce type d'approche ? Est-ce un domaine où toute application de l'intelligence artificielle serait vaine ? Une analyse plus fine de la faillite américaine montre que les militaires et les analystes n'ont pas assez réfléchi aux enjeux de la guerre au Vietnam. Ils privilégièrent la quantité des indicateurs à la qualité et la sélection de quelques marqueurs appropriés reflétant mieux l'évolution de la guerre. Les Américains furent de ce fait submergés, incapables de traiter correctement la masse d'informations qu'ils accumulèrent. L'immobilisme bureaucratique des états-majors et la rotation régulière des cadres qui nuisait à leur investissement empêchèrent de remettre en cause les

42. G. A. Daddis, *No Sure Victory: Measuring US Army Effectiveness and Progress in the Vietnam War*, New York, Oxford University Press, 2011.
43. H. G. Summers, *On Strategy: A Critical Analysis of the Vietnam War*, New York, Presidio Press, 1984, p. 18.
44. D. Kinnard, *The War Managers*, New Hampshire, Hanover, 1977, p. 73, cité *in* D. F. Harrison, « Computers, Electronic Data and the Vietnam War », *Archivaria*, vol. 26, été 1988, p. 18-32.
45. G. A. Daddis, *No Sure Victory, op. cit*, p. 226.

paramètres déjà sélectionnés. Une routine fatale s'installa, que chacun s'appliquait à reproduire[46].

Cependant, le témoignage d'Enthoven relativise certains clichés. Il est lui-même critique de l'usage du *body count*. La saisie de documents ennemis avait montré l'imprécision des estimations américaines sur les pertes de leur adversaire. Selon lui, « le problème ne fut pas un trop grand nombre d'analyses, ce fut qu'il n'y en eut pas assez[47] ». Ce qui manqua le plus fut de donner du sens aux données quantifiées. Peu importait que ces données ne soient pas précises, car elles ne le sont finalement que rarement en temps de guerre. Elles pouvaient néanmoins suggérer des modèles assez consolidés pour refléter les stratégies opposées et pour indiquer les progrès qu'accomplissaient les deux camps, pourvu qu'on fasse l'effort de les traduire[48]. Une des leçons de cette guerre n'est donc pas que l'approche statistique ait été mauvaise, mais plutôt qu'aucun expert n'ait su l'appréhender de manière pertinente[49]. L'aide de l'intelligence artificielle à la stratégie militaire ne doit donc pas être condamné *a priori*.

Les applications militaires à court terme

À la manière des applications civiles, les programmes militaires faisant appel à l'intelligence artificielle se multiplient aujourd'hui. Michael Griffin, sous-secrétaire de la Défense à la recherche et l'ingénierie, déclarait le 18 avril 2018 devant la Commission des forces armées de la Chambre des représentants que le Département de la Défense comptait 592 projets intégrant une forme plus ou moins évoluée d'intelligence artificielle[50]. Le panorama rapide proposé ici ne saurait donc prétendre à l'exhaustivité, mais vise à évoquer certaines applications déjà utilisées par les forces ou en cours de développement. Cela permet de mieux apprécier les domaines qui seront affectés à l'avenir par le développement de cette nouvelle technologie. L'ensemble des tâches concernées reste très spécifique et aucun usage d'« intelligence forte » n'est pour l'instant sérieusement évoqué.

46. La lecture de l'ouvrage de G. A. Daddis est fondamentale pour illustrer ce processus.
47. A. C. Enthoven et K. Wayne Smith, *How Much is Enough? Shaping the Defense Program, 1961-1969*, New York, Harper & Row, 1971, p. 88 cité *in* D. F. Harrison, « Computers, Electronic Data and the Vietnam War », *Archivaria*, vol. 26, été 1988, p. 23.
48. D. F. Harrison, « Computers, Electronic Data and the Vietnam War », *op. cit*, p. 22-23.
49. L'approche actuellement la plus stimulante dans l'utilisation des données de masse dans un cadre de contre-insurrection se trouve dans E. Berman, J. H. Felter et J. N. Shapiro, *Small Wars, Big Data: The Information Revolution in Modern Conflict*, Princeton, Princeton University Press, 2018.
50. A. Mehta, « Pentagon Developing Artificial Intelligence Center », *C4ISRNET*, 18 avril 2018, disponible sur : www.c4isrnet.com.

Gérer et simuler l'environnement

L'utilisation directe de logiciels civils peut d'abord s'avérer fructueuse pour les militaires en opération. Les programmes de traduction ont une utilité évidente pour les soldats au contact d'une population ou de partenaires étrangers ou pour des membres des forces spéciales, progressant de manière autonome dans des régions où seuls les dialectes locaux sont usités.

Par ailleurs, l'IA peut se révéler être un outil performant pour s'adapter à un environnement mal connu ou complexe. La définition de la meilleure route pour se rendre d'une base militaire vers un endroit précis dans une mégapole mal connue pourrait être calculée dans des temps très courts grâce à des logiciels inspirés par exemple de *Waze*. Des chemins préférentiels pourraient même être proposés en fonction de l'intégration d'une situation tactique ou de la prise en compte de la présence probable d'*Improvised Explosive Device* (IED).

Pour ce qui touche à la préparation au combat, des jeux de guerre employant des IA encore limitées existent déjà. Le logiciel SWORD du groupe MASA permet par exemple de simuler les réactions d'un ennemi au cours d'un affrontement terrestre[51]. Les unités adverses se comportent néanmoins selon des guides très précis. Elles suivent fidèlement les principes de leurs doctrines, qui commandent leurs mouvements et leurs réactions face aux événements.

Détecter et traiter

L'un des champs où l'IA s'impose de plus en plus est toutefois celui de la détection et du traitement automatisé de données. Des sons émis par des navires de guerre, des sous-marins, des avions ou des engins militaires peuvent être recueillis, analysés et attribués avec une précision supérieure à celle des meilleurs analystes humains. Mais les données traitées peuvent appartenir à d'autres catégories, comme un texte, des grandeurs physiques, ou même des images d'objets ou d'êtres humains.

L'intelligence artificielle peut ainsi parcourir des dizaines de milliers de documents pour rechercher des informations spécifiques. Des logiciels adaptés traquent des mots-clés, des expressions, des acronymes et sont capables de les extraire automatiquement. Le programme Maurdor de la Direction générale de l'armement (DGA) semble être développé en ce sens[52]. La possibilité de recouper différentes sources et d'associer des

51. La présentation de ce logiciel est disponible sur : masa-group.biz.
52. Définition disponible sur : www.maurdor-campaign.org.

informations peut s'avérer très fructueuse pour dévoiler des liens entre des notions *a priori* sans connexion[53].

Un autre domaine réside dans l'optimisation des opérations de maintenance. Des données représentatives sont recueillies pour définir l'état de fonctionnement des systèmes d'un navire, d'un avion ou d'un véhicule terrestre, comme des températures ou des pressions pour les moteurs. Elles sont comparées aux grandeurs obtenues précédemment et analysées par rapport aux valeurs nominales de fonctionnement. En fonction des tendances, il est possible d'anticiper les pannes. Les pièces défectueuses pourront être remplacées avant que le système ne défaille. Les phases nécessaires de réparation ou de régénération du matériel pourront être anticipées et la manœuvre adaptée en conséquence en fonction des prévisions de disponibilité.

Les comportements « anormaux » peuvent être traqués de la même manière pour tout ce qui touche à la cybersécurité. Des bases d'apprentissage sont notamment constituées avec l'exploitation massive de rapports d'activité ou des fichiers de logs, qui indiquent l'historique des événements. Les anomalies sont ainsi répertoriées. Des bases de données extérieures peuvent compléter ces éléments. L'intelligence artificielle est alors capable de construire des modèles représentant statistiquement des menaces et même d'en détecter d'inédites, améliorant la sécurité des réseaux informatiques[54].

L'« analyse comportementale » appliquée à des bâtiments ou des véhicules peut également donner des résultats. Des infrastructures sensibles peuvent être reconnues en fonction d'activités anormales effectuées par des spécialistes déjà identifiés. Des véhicules peuvent être suivis et leurs parcours analysés pour mieux se renseigner sur les déplacements de son propriétaire, sur ses habitudes, sur ce qui constitue son « *pattern of life* ».

Les êtres humains constituent également des cibles de choix. Les applications de reconnaissance faciale sont encore limitées dans le civil. Elles offrent par exemple la possibilité au propriétaire d'un téléphone portable d'être le seul à pouvoir déverrouiller son appareil après que la caméra intégrée l'ait reconnu[55]. L'intérêt militaire ou sécuritaire de tels logiciels semble beaucoup plus vaste. Des dispositifs de reconnaissance placés sur des

53. Entretien avec un expert militaire.
54. T. Berthier, « Les apports de l'intelligence artificielle en cybersécurité et cyberdéfense », *Deftech*, n° 1, juin-août 2018, p. 39.
55. Un logiciel de reconnaissance faciale simple peut identifier 80 points nodaux sur le visage. Lire à ce sujet : M. Rouse, « Facial Recognition », *SearchEnterpriseAI*, janvier 2018, disponible sur : searchenterpriseai.techtarget.com.

armes n'autoriseraient leur utilisation que par leur propriétaire ou les membres d'une même unité. L'IA peut par ailleurs reconnaître et identifier des visages dans des lieux publics et très fréquentés. Dans un contexte de contre-terrorisme, des capteurs peuvent scanner une foule à partir d'un renseignement pour trouver la personne recherchée. Elle peut être neutralisée ou suivie pour repérer les autres activistes qu'elle rencontre. Le marché de la surveillance des individus est ainsi en plein développement et suscite beaucoup d'intérêt chez les responsables politiques, notamment dans les régimes autoritaires. L'intelligence artificielle peut malheureusement être d'une grande aide pour recenser les personnes participant à des manifestations ou repérer les comportements jugés « déviants ». En Chine, les compagnies *Sensetime* et *Megvii*, en pointe dans ce domaine, ont dépassé le milliard de dollars de valorisation[56].

Simplifier

Trouver la bonne information parmi toutes les données disponibles peut être cependant une gageure avec l'usage exponentiel des caméras au sol ou dans les airs. En 2011, l'*US Air Force* a par exemple recueilli 325 000 heures de vidéo à partir des caméras embarquées sur ses drones, soit l'équivalent de 37 années de projection pour un seul analyste image[57]. Ces chiffres ont nettement augmenté depuis. Les opérateurs peuvent manquer un événement notable pendant leurs longues heures de surveillance par un manque de concentration ou même ne pas pouvoir consulter l'ensemble des scènes filmées par manque de temps. L'intelligence artificielle offre des solutions innovantes pour pallier ces limites humaines. Le projet *Maven* a été lancé en ce sens en 2017 par Robert Work. Il s'agit dans un premier temps d'utiliser des algorithmes de reconnaissance dans un contexte opérationnel pour la détection, la classification et le signalement d'objets[58]. Mis en œuvre dès la fin 2017 dans le plan de frappes contre l'État islamique en Irak et en Syrie, les logiciels sont parvenus à reconnaître dans 80 % des cas les personnes, véhicules ou bâtiments recherchés[59].

56. E. Trujillo, « En Chine, le grand bond en avant de la reconnaissance faciale », *Le Figaro*, 13 décembre 2017.
57. T. Johnson et C. F. Wald, « The Military Should Teach AI to Watch Drone Footage », *Wired*, 26 novembre 2017, disponible sur : www.wired.com.
58. « Establishment of an Algorithmic Warfare Cross-Functional Team (Project Maven) », *Memoradum*, Deputy Secretary of Defense, Washington D. C., 26 avril 2017, disponible sur : www.govexec.com
59. M. Weisgerber, « The Pentagon's New Artificial Intelligence Is Already Hunting Terrorists », *Defense One*, 21 décembre 2017, disponible sur : www.defenseone.com.

Comme dans le cas de l'optimisation de la maintenance, les vidéos les plus récentes pourront être comparées à terme avec d'autres plus anciennes pour savoir si l'environnement a changé, si des modifications significatives sont advenues dans un laps de temps donné. Cette comparaison pourrait se faire dans le capteur lui-même, afin de limiter le volume du transfert de données et d'économiser sensiblement l'utilisation de la bande passante disponible. Des données plus directement utiles pourraient donc être mises à disposition directe des opérateurs dans l'avenir grâce à l'intelligence artificielle[60].

Automatiser

Outre la détection et le tri des données, l'intelligence artificielle va profondément affecter l'automatisation de certaines tâches dans les systèmes informatiques. Le projet *Consolidated Afloat Networks and Enterprise Services* (CANES) de l'*US Navy* illustre cette tendance[61]. La multiplication des réseaux informatiques est indispensable pour le fonctionnement des systèmes perfectionnés et complexes, mais elle est aussi une source de vulnérabilité. Le porte-avions *USS Truman* comprend par exemple 3 400 réseaux locaux répartis sur plus de 2 700 localisations différentes dans le navire. L'IA va automatiser la surveillance de ces systèmes pour vérifier leur bon fonctionnement et se prémunir contre les menaces cyber, avec la possibilité de produire des patchs de protection quand une menace est détectée. CANES doit également améliorer la coordination des feux entre les bâtiments d'une flotte. Les logiciels s'appuieraient sur la fusion des données recueillies par l'ensemble des capteurs d'un groupe naval pour suggérer des solutions de tir optimisées, tenant compte de l'état et de la position des systèmes d'arme sur les différents navires.

Prédire

Néanmoins, le programme le plus ambitieux et le plus intrigant, car il aspire à défier directement les stratèges humains, est probablement le *Collection and Monitoring via Planning for Active Situational Scenarios* (COMPASS)[62]. Son but est de fédérer, grâce à l'intelligence artificielle, plusieurs disciplines comme la théorie des jeux, la modélisation ou la

60. T. Johnson et C. F. Wald, « The Military Should Teach AI to Watch Drone Footage », *op. cit.*
61. E. Chiva, « Une bonne année et pour commencer : intelligence artificielle et combat naval », *VMF 214*, 2 janvier 2018, disponible sur : vmf214.net. L'*US Navy* investit 2,5 milliards de dollars dans ce système.
62. P. Tucker, « The Pentagon Wants IA To Reveal Adversaries' True Intentions », *Defense One*, 16 mars 2018, disponible sur: www.defenseone.com.

simulation pour tenter de deviner les intentions d'un adversaire dans un conflit limité éclatant dans une « zone grise[63] ». COMPASS tente plus précisément d'identifier la manière dont l'ennemi pourrait agir dans telle ou telle situation. Comme pour le poker, il s'agit moins de lire dans le cerveau de l'adversaire que de prendre en compte le maximum d'hypothèses et de limiter les risques. Les nouveaux algorithmes doivent être capables d'extraire les données les plus remarquables d'une vaste gamme de sources de différents types (vidéo, texte, image, etc.) déjà disponibles, mais mal ou peu exploitées. Aucun investissement supplémentaire dans des capteurs n'est prévu.

Au terme de cette brève revue de quelques applications militaires de l'intelligence artificielle, on constate avec Michael C. Horowitz que celle-ci est tout sauf une nouvelle arme[64]. C'est un facilitateur (*enabler* en anglais), qui se rapproche plus d'inventions comme l'électricité ou le moteur à combustion que de l'avion de chasse ou du char de combat. Réfléchir aux applications militaires de l'intelligence artificielle revient donc à s'interroger sur la manière dont elle pourrait améliorer et structurer les processus, les tactiques, les stratégies ou les différentes fonctions que les militaires doivent remplir. Elle ne s'incarnera pas dans une machine qui dominera le champ de bataille grâce à des performances remarquables et inédites.

La poursuite de la Révolution dans les affaires militaires

L'introduction de l'intelligence artificielle dans les armées s'inscrit dans un processus doctrinal commencé pendant la guerre froide, qui a pris aux États-Unis la forme de stratégies de compensation (*Offset Strategy*) successives. Ces stratégies naissent à chaque fois que les élites américaines perçoivent une infériorité militaire, ou au moins un rapport de force qui n'est pas en leur faveur face à des adversaires réels ou potentiels. Dans les années 1950 d'abord, les Américains constatent qu'ils ne disposent pas de la supériorité conventionnelle face aux Soviétiques sur le théâtre européen, du fait d'un large avantage quantitatif des forces communistes. L'administration Eisenhower ne désirant pas relancer les dépenses militaires, les États-Unis décident de compenser leur infériorité numérique par la mise en place d'armes nucléaires tactiques qui doivent empêcher par

63. Un conflit dans une « zone grise » étant défini ici sommairement comme un affrontement entre des acteurs étatiques et non étatiques, avec un niveau d'intensité inférieur à celui d'un conflit conventionnel.

64. M. C. Horowitz, « The Promise and Peril of Military Applications of Artificial Intelligence », *Bulletin of the Atomic Scientists,* 23 avril 2018, disponible sur : thebulletin.org. M. C. Horowitz est un chercheur américain en sciences politiques.

exemple la concentration des unités soviétiques pour percer les défenses de l'OTAN. C'est la première stratégie de compensation.

La deuxième stratégie de compensation est étroitement associée à la Révolution dans les affaires militaires (RMA selon l'acronyme anglais)[65]. Cette « révolution » correspond en fait aux évolutions militaro-technologiques suscitées par le développement des technologies de l'information et de l'armement guidé. Alors que la puissance américaine se relève péniblement du revers vietnamien, elle doit affronter un adversaire soviétique en expansion dans le Tiers-monde, qui déploie en Europe une nouvelle génération de missiles nucléaires de moyenne portée et entretient sa supériorité conventionnelle. Les stratèges américains choisissent d'investir dans la montée en gamme technologique de leurs équipements, en informatisant leurs forces, en valorisant les réseaux d'information et en introduisant les munitions de précision. Leur choix se révèle payant : l'armée irakienne est balayée lors de la guerre du Golfe tandis que la Chine et la Russie sont incapables de rivaliser sur le terrain militaire avec les États-Unis pendant deux décennies.

L'émergence des problématiques de déni d'accès marque le retour de la contestation de la supériorité américaine par Moscou et Pékin[66]. Les militaires russes et chinois ont adopté et intégré ces nouvelles technologies à leurs ambitions stratégiques et peuvent gêner considérablement la projection des éléments américains sur des zones de tension ou de guerre. Face à ce défi, le Pentagone décide d'appliquer à nouveau la recette qui a fonctionné en identifiant des solutions technologiques innovantes pour résoudre les problèmes tactiques et en pariant sur leur intégration rapide dans les forces armées. Cette nouvelle RMA prend le nom de « Troisième stratégie de compensation » (*Third Offset Strategy* – TOS) au milieu des années 2010. Elle est particulièrement défendue et valorisée par Robert Work. Comme celui-ci l'explique lors d'une intervention publique en octobre 2016, l'impulsion initiale est d'exploiter toutes les avancées dans les domaines de l'autonomie pour assurer une forte amélioration des performances et réaffirmer la dissuasion conventionnelle[67].

65. Voir notamment A. F. Krepinevich, « Cavalry to Computer: The Pattern of Military Revolutions », *The National Interest*, n° 37, automne 1994, p. 30-42 ; E. A. Cohen, « A Revolution in Warfare », *Foreign Affairs*, mars-avril 1996, p. 37-54.
66. A. F. Krepinevich et B. Watts, *Meeting the Anti-Access and Area-Denial Challenges*, Center for Strategic and Budgetary Assessment, Washington D. C., 20 mai 2003 ; C. Brustlein, « Vers la fin de la projection de force ? I. La menace du déni d'accès », *Focus stratégique,* n° 20, Ifri, avril 2010, disponible sur : www.ifri.org.
67. Les propos de l'intervention sont disponibles sur ce lien : www.csis.org.

L'intérêt stratégique de l'intelligence artificielle doit permettre de maintenir ou retrouver un écart entre les capacités des armées américaines et celles de leurs adversaires potentiels pour empêcher tout risque de lutte à armes égales (*fair fight*). Il n'est pas concevable de mettre en danger la vie des citoyens/soldats américains ou de risquer l'échec alors que des alternatives existent. La supériorité dans le domaine conventionnel, obtenue grâce à l'intelligence artificielle, doit être telle qu'aucune autre puissance ne pourra envisager de défier les forces américaines sur le champ de bataille sans s'exposer à coup sûr à la débâcle.

Les liens qui unissent la RMA et la TOS ne se limitent pas à un processus et un but commun. La seconde tente de prolonger et d'élargir les résultats obtenus par la première. L'amiral William Owens, V*ice Chairman of the Joint Chiefs of Staff*[68], espérait que les opérateurs américains, grâce à une bonne répartition des capteurs, puissent avoir une connaissance parfaite des opérations amies et ennemies en cours dans un carré de 350 kilomètres de côté[69]. Ce discours reste d'actualité, mais la TOS est en même temps plus ambitieuse que la RMA. La gamme des données compilées à terme ne se bornera pas au cadre spatial et temporel du champ de bataille mais convoquera également les sciences humaines, avec l'intégration de paramètres psychologiques, d'éléments sociologiques, et de capacités économiques. Il prendra en compte les doctrines, les manières de travailler et de raisonner des chefs ennemis. Il s'inscrira dans la durée plutôt que dans l'instant présent. Les données tactiques actuelles seront interprétées en comparaison avec d'autres, plus anciennes, ce qui caractérisera le sens de leur évolution et permettra d'agir plus finement. Le stratège aura accès à une plus large quantité d'informations utiles, qui éclaircira plus ou moins le brouillard de la guerre selon les circonstances.

De même, la RMA présentait l'avantage d'importer les informations traitées immédiatement vers les tableaux de bord des opérateurs de systèmes d'armement, de sorte que ceux-ci pouvaient rapidement neutraliser la cible s'ils en avaient l'autorisation. Avec la TOS, il ne s'agit plus seulement d'être en capacité de tirer promptement sur une cible. L'art de la guerre dans son ensemble va dépendre qualitativement de la vitesse d'exécution des algorithmes, au travers de leur capacité à traiter instantanément les informations reçues et à présenter les meilleures options. Le cerveau humain n'imposera plus son rythme pour certaines tâches. L'étalon de mesure sera notamment celui de la puissance des processeurs, pouvant transférer à la vitesse de la lumière des instructions

68. Vice-chef d'état-major des Armées. Cette fonction n'existe pas dans l'armée française.
69. M. R. Gordon, « Admiral with High-Tech Dreams Has Pentagon at War With Itself », *The New York Times*, 12 décembre 1994.

vers d'autres ordinateurs ou opérateurs à des fins d'identification, de prédiction, de décision ou d'action.

Une évolution de la tactique se dessine. Le « *Search and Destroy* » du Vietnam, où un effort important devait être consenti pour trouver l'ennemi, le fixer avant de le détruire, et où les deux fonctions de reconnaissance et de combat étaient séparées, est devenu avec la RMA le « *See it, Shoot it*[70] ». La simple détection peut se révéler fatale car le tir peut être déclenché. Dorénavant, il faudra peut-être employer l'expression « *Find it, Manage it* » – trouve-le, gère-le – pour caractériser l'âge de l'intelligence artificielle. La recherche d'informations se traduira par des résultats suffisants pour mieux connaître son adversaire et envisager une variété de modes d'action pour lui imposer sa volonté, allant de la surveillance à la destruction.

Quelle influence sur la préparation des forces et les opérations ?

S'il paraît possible d'imaginer la direction des nombreuses applications militaires de l'IA et leur impact sur la tactique, il est moins aisé de saisir spontanément les stratégies que cette dernière va favoriser. La description de ces stratégies potentielles dans les paragraphes qui suivent suppose le développement d'intelligences artificielles faibles, mais avec des capacités supérieures à celles d'aujourd'hui et connectées entre elles. Par ailleurs, elles ne constituent pas une recette à suivre ou à dérouler pour parvenir au but désiré. La stratégie est une activité humaine bien trop complexe pour uniquement dépendre des performances d'une technologie. Elles pourraient cependant être les plus adaptées pour profiter pleinement du potentiel de l'intelligence artificielle.

Améliorer l'entraînement, la simulation et la conception des équipements

L'IA va d'abord jouer un rôle dans la préparation des forces, en améliorant sensiblement l'entraînement des soldats. Elle pourra s'adapter au niveau des opérateurs pour les aider à mieux maîtriser les systèmes d'arme. Si un pilote a par exemple plus de difficultés à assimiler certaines tâches, une intelligence artificielle pourra insister sur ces points en proposant des exercices originaux et adaptés et passer plus rapidement sur des domaines où il présente de meilleures aptitudes. L'IA pourra également introduire dans les simulations la présence de forces adverses, saisir la manière dont

70. C. J. Fuller, *See It/Shoot It: The Secret History of the CIA's Lethal Drone Program*, New Haven, Yale University Press, 2017.

l'opérateur tend à réagir face aux initiatives ennemies et le défier à chaque fois différemment, en apportant des variantes en fonction de ses points faibles.

La simulation pourra aussi être améliorée au niveau de la planification opérative. Les officiers pourront se confronter de manière fructueuse avec une IA « ennemie », à l'image de celles des jeux vidéo actuels, mais avec des capacités bien supérieures. Des modes d'action pourront être testés pour juger de leur validité. L'IA « ennemie » apprendra encore une fois la manière dont fonctionne l'état-major en charge de la planification et pourra tenter de le surprendre. D'éventuels revers face aux logiciels permettront d'anticiper différentes évolutions des opérations et de faire face plus aisément aux épreuves. L'IA sera d'une grande aide pour sélectionner les meilleures stratégies et, le cas échéant, adapter l'organisation des unités pour produire les effets recherchés.

La conception des équipements pourra également bénéficier des atouts de l'IA, en faisant varier lors de simulations au niveau opératif différents modèles avec des performances et des caractéristiques variées. Alors que les matériels sont principalement testés dans un environnement tactique lors des phases de développement, leurs prouesses pourront être jugées dans des dispositifs plus larges face à des adversaires réactifs au cours de simulations inédites.

Accélération du rythme des opérations

L'un des apports de la RMA a été de démontrer le lien direct entre domination informationnelle et efficacité militaire. Cette relation a notamment été illustrée au travers du concept de boucle OODA (Observation, Orientation, Décision, Action) imaginé par l'aviateur américain John Boyd[71]. Cette boucle décompose de manière synthétique le processus de décision appliqué par un pilote de chasse en combat aérien. Celui-ci observe les évolutions de l'avion adverse, s'oriente vers la meilleure position possible, prend la décision finale et enfin déclenche son tir. Le fonctionnement de cette boucle a été étendu par Boyd à celui de toute organisation confrontée à une tâche à accomplir.

La supériorité informationnelle issue de la RMA se traduit par un parcours plus rapide de la boucle, notamment des deux premières phases. Il est alors possible de réagir plus rapidement aux événements et de pénétrer en quelque sorte dans le cycle de décision de son ennemi. Cet

71. G. T. Hammond, *Col. John R. Boyd: A Discourse On Winning and Losing*, Maxwell AFB, Air University Press, 2018. OODA désigne quatre périodes successives correspondant à l'observation, l'orientation, la décision et enfin l'action.

avantage comparatif offre en théorie la maîtrise du *tempo* des opérations. Une telle supériorité peut favoriser la mise en œuvre de nombreux modes d'action, fondés par exemple sur le cadencement des attaques dans le temps ou au contraire leur synchronisation selon les effets souhaités. Elle encourage la prise d'initiative, en devançant les intentions de l'ennemi ou en lui imposant les siennes. Des opportunités peuvent en outre être saisies, comme neutraliser une cible à haute valeur ajoutée, qui vient juste d'être identifiée. Elle permet enfin d'agir au bon moment, au bon endroit, ce qui permet de mobiliser en un lieu donné du champ de bataille le nombre juste suffisant d'unités, et de susciter en retour une économie des moyens.

L'intelligence artificielle sera décisive pour promouvoir de telles stratégies, puisqu'elle sera capable d'accomplir les phases d'observation et d'orientation de la boucle OODA plus vite et en principe plus efficacement que n'importe qui. Elle pourrait accélérer significativement le rythme des opérations, faisant émerger une nouvelle version de la guerre-éclair, où l'adversaire, étouffé, passif, n'aura d'autres options que subir la volonté de son ennemi. L'intelligence artificielle favorisera sans aucun doute l'attaque dans l'avenir, en fragilisant les tactiques de retardement, de déni (au travers des fortifications, de la dispersion et du camouflage) et de manœuvre du défenseur[72]. La maxime de Clausewitz qui affirme que la défense est la forme la plus forte de conduite de la guerre pourrait ainsi être invalidée.

L'incertitude continuera bien sûr de régner sur le champ de bataille et le désordre, le chaos reviendront dès que le combat s'engagera. Mais pour certains responsables, le « coup d'œil » des commandants militaires sera largement amélioré par l'intelligence artificielle. Ils pourront mieux saisir le déroulement des événements, comprendre l'évolution de la situation et infléchir en cas de besoin la direction de leur manœuvre[73]. S'adapter aux aléas de la bataille pour improviser et innover deviendra des tâches plus simples.

Les algorithmes d'intelligence artificielle sont d'autant plus performants qu'ils doivent analyser un système comprenant un nombre d'objets limités, agissant selon des règles fixes et établies, avec des interactions restreintes. Moins le niveau de complexité est élevé et plus les prévisions et les résultats seront convenables. À ce titre, les milieux maritime et aérien offrent des opportunités remarquables pour l'emploi de l'IA qu'il est plus difficile d'atteindre dans le milieu terrestre où la présence

72. K. Payne, *Strategy, Evolution, and War: From Apes to Artificial Intelligence*, Washington D. C., Georgetown University Press, 2018, p. 20-21.
73. S. J. Freedberg Jr., « War Without Fear: DepSecDef Work on How AI Changes Conflict », *Breaking Defense*, 31 mai 2017 , disponible sur : breakingdefense.com.

des hommes, civils ou combattants, multiplie les interactions et complique les calculs et les prévisions. Le nombre d'aéronefs ou de navires de guerre demeure limité. Les règles d'emploi peuvent varier, mais elles dépendent de lois physiques comme la gravité ou le frottement des mobiles dans l'air ou dans l'eau. Les performances des moteurs, les portées des missiles, l'autonomie des vecteurs sont connus et peuvent être intégrées. La modélisation, si elle n'est pas aisée, est plus simple.

Il n'est donc pas surprenant qu'une intelligence artificielle surnommée ALPHA, qui fit ses classes en affrontant des programmes informatiques de combats aériens de l'*Air Force Research Lab*, ait systématiquement triomphé d'un ancien pilote de chasse chevronné lors d'une succession de simulations d'engagements aériens simulés en octobre 2015[74]. Le pilote déclara qu'il fut surpris :

> « [...] de la manière dont [ALPHA] était attentive et réactive. Elle semblait consciente de mes intentions et réagissait instantanément à mes initiatives et au départ de mes missiles. Elle savait comment contrer les tirs que je faisais. Elle passait instantanément d'un mode défensif à un mode offensif quand il y avait besoin. [...] Un pilote expérimenté peut battre [la plupart des autres IA] s'il sait ce qu'il fait. C'est sûr, il se pouvait que vous soyez abattu une fois de temps en temps par une IA quand [...] vous essayiez quelque chose de nouveau, mais, jusqu'à maintenant, une IA ne pouvait tenir le rythme [...] dans des scénarios de combat aérien.[75] »

Ajoutons que d'autres pilotes ont connu la même mésaventure lors de séances de simulateur qui se sont tenues par la suite. Pire, ALPHA continua de triompher dans des cas où ses logiciels commandaient une plateforme virtuelle délibérément diminuée, avec des performances moindres en termes de vitesse, de détection ou de tir. Même si tous les détails de cette expérimentation ne sont pas dévoilés, l'issue du combat paraît moins surprenante quand on apprend que l'intelligence artificielle pouvait examiner les différentes options tactiques et proposer des réponses adéquates 250 fois plus vite que ses adversaires humains. Pourtant, elle fonctionnait avec la puissance de calcul d'un nano-ordinateur monocarte qui était vendu à seulement 35 dollars[76]...

74. N. Ernest, D. Carroll, C. Schumacher, M. Clark, K. Cohen et G. Lee, « Genetic Fuzzy Based Artificial Intelligence for Unmanned Combat Aerial Vehicle Control in Simulated Air Combat Missions », *Journal of Defense Management*, vol. 6, n° 1, 2016.
75. M. B. Reilly, « Beyond Video Games: New Artificial Intelligence Beats Tactical Experts in Combat Situation », *UC Magazine*, 27 juin 2016.
76. *Ibid*.

Les conséquences stratégiques de cette supériorité tactique – qui reste à démontrer à l'extérieur des murs d'un simulateur – sont importantes. L'IA peut être une composante essentielle dans l'avenir pour vaincre sur la mer, dans les airs, ou dans d'autres milieux comme l'espace ou le cyberespace. Le résultat positif de chaque duel participera progressivement à la défaite du camp mettant en œuvre les IA les moins performantes ou ne faisant confiance qu'à l'homme. Un modèle émerge, qui renforce les contours du schéma qui s'est imposé au niveau opératif dans les forces armées occidentales depuis 1945. La victoire se dessine d'abord sur mer, dans les airs et ajoutons maintenant, dans l'espace et le cyberespace. Une fois la supériorité acquise dans ces milieux, il est possible d'agir sur la terre et d'exploiter les opportunités offertes par cette prédominance pour des opérations de coercition.

Vers l'hyperpersonnalisation de la guerre ?

Les grandes formations terrestres pourraient aussi devenir à terme les victimes du développement de l'intelligence artificielle. Plutôt, l'ensemble des unités s'appuyant sur des corpus doctrinaux précis, sur la mise en place de procédures contraignantes pour coordonner et harmoniser leurs actions, peut être en danger. À la manière d'un Jomini qui, de par sa connaissance personnelle de Napoléon, a suggéré aux forces alliées le plan devant amener à la défaite de l'empereur en 1814, une IA suffisamment forte pourrait lire les intentions et déchiffrer le sens des manœuvres répondant à des exigences strictes[77]. En outre, la lourde logistique nécessaire au fonctionnement de ces unités massives ajoute à leur vulnérabilité. Des intelligences artificielles pourraient identifier précisément les nœuds des réseaux de ravitaillement et d'approvisionnement et proposer de les détruire pour paralyser toute manœuvre ou action.

À l'autre extrémité du spectre, les individus semblent les cibles les plus accessibles et peut-être les plus faciles à influencer[78]. Le scandale *Cambridge Analytica* a montré par exemple l'usage qui pouvait être fait du détournement de données personnelles de 87 millions d'utilisateurs de Facebook à des fins de propagande électorale hyperpersonnalisée rendant possible un ciblage d'électeurs potentiels dont il s'agissait de s'assurer de

77. H. Houssaye, *1814 : la campagne de France,* Etrépilly, C. de Bartillat, 1991, p. 651.
78. J.-B. Jeangène Vilmer, A. Escorcia, M. Guillaume et J. Herrera, *Les manipulations de l'information : un défi pour nos démocraties*, rapport du Centre d'analyse, de prévision et de stratégie (CAPS) du ministère de l'Europe et des Affaires étrangères et de l'Institut de recherche stratégique de l'École militaire (IRSEM) du ministère des Armées, Paris, août 2018 ; J. Henrotin, « Les mutations du renseignement militaire. Dissiper le brouillard de la guerre ? », *Focus Stratégique*, n° 71, Ifri, janvier 2017, disponible sur : www.ifri.org.

la bonne mobilisation. D'un point de vue sécuritaire, l'IA peut ainsi être employée dans une logique d'action d'influence, voire de guerre psychologique pour influencer massivement une population adverse, ou au contraire galvaniser ses propres masses. La surveillance des opinions subversives en vue d'assurer la « solidité des arrières » est aussi un usage stratégique à portée de main à l'instar de ce qui semble d'ores et déjà en marche en Chine avec le système du « crédit social[79] ». En cas de crise, un tel État pourrait élaborer des messages personnalisés pour certains individus civils ou militaires ciblés.

À l'échelon tactique, ce type d'usage peut être exploité pour intoxiquer les membres d'une unité en particulier, en l'incitant par exemple à dévoiler sa position ou même à se rendre ou déserter. À l'échelon stratégique, il peut s'agir de cibler des relais d'opinion chez l'adversaire en les incitants à diffuser des fausses nouvelles et à semer la discorde sur ses arrières. Ces messages seraient élaborés à la manière des offres commerciales qui sont façonnées pour donner envie de consommer en fonction de l'historique de nos dépenses. Ils seraient construits à partir du profil-type que nous dégageons, de la fréquentation de certains sites, de l'appartenance à certains réseaux sociaux, de la sensibilité des uns et des autres. Leurs contenus insisteraient sur le bon droit d'un État à prendre certaines initiatives ou souligneraient au contraire des éléments fragilisant la légitimité des gouvernements qui s'opposent à ses desseins.

Le recueil d'informations sur les individus pourrait aussi prendre de plus en plus d'importance dans les opérations de contre-insurrection, avec l'enregistrement de caractéristiques biométriques pour mieux apprécier si des habitants locaux sont impliqués dans des actions hostiles. Par ailleurs, des efforts pourraient être consentis pour mieux appréhender les individus qui pourraient tenir des postes à responsabilité dans les organisations militaires ou politiques adverses. L'intelligence artificielle pourrait repérer des comportements réguliers, des conduites répétées qui permettraient d'anticiper certaines réactions. Appréhender dans le temps les forces et les vulnérabilités de ces individus, la manière dont ils décident, dont ils gèrent le stress, dont ils agissent au sein d'une bureaucratie pourrait s'avérer très utile si les circonstances plaçaient de tels hommes dans des postes à responsabilité lors d'un conflit. L'intelligence artificielle pourrait ainsi donner un nouvel essor à ce que le général américain Charles Dunlap avait nommé en 2014

79. A. Mitchell et L. Diamond, « China's Surveillance State Should Scare Everyone », *The Atlantic*, 2 février 2018 ; C. Rolet, « The Odd Reality of Life under China's All-Seeing Credit Score System », *Wired*, 5 juin 2018, disponible sur : www.wired.co.uk.

l'hyperpersonnalisation de la guerre en évoquant l'arsenalisation du *big data* et ces conséquences sur les individus[80].

Finalement, il est probable que l'intelligence artificielle faible ne révolutionne pas la guerre, mais qu'elle amplifie les orientations stratégiques déjà prises. Elle favoriserait l'offensive et une accélération du rythme des opérations. Elle pourrait se révéler particulièrement décisive dans les milieux où l'homme peut évoluer grâce à des artifices technologiques, mais où il ne vit pas, où il n'interagit pas avec le milieu ou avec d'autres hommes de manière durable. L'individu pourrait devenir une cible privilégiée, car plus facilement isolable.

80. C. J. Dunlap Jr., « The Hyper-Personalization of War: Cyber, Big Data and the Changing Face of Conflict », *Georgetown Journal of International Affairs*, 2014, p. 108-118.

Une relation homme-machine transformée

Vers l'automatisation comme norme ?

Si la prise en compte d'un plus grand nombre de données offre des possibilités d'analyse encore impensables il y a peu, si les capacités croissantes des calculateurs entraînent l'accélération du rythme des opérations, la place de l'homme dans ce nouveau contexte pose question. En effet, le *tempo* de la guerre se mesure d'abord à l'aune des capacités cognitives des hommes. Les cadres militaires décident selon des processus élaborés pour correspondre à leurs facultés. Un temps incompressible existe toujours pour l'analyse de la situation et pour le choix du mode d'action. Les durées peuvent même s'allonger si la situation est complexe ou s'il faut appréhender soudainement des événements imprévus. Les ordres sont initialement transmis par la voix ou par écrit, avant d'être diffusés électroniquement. Ils doivent être bien compris par les subordonnés, ce qui retarde le moment de l'exécution. Les soldats agissent enfin sur le champ de bataille selon leur perception des événements.

Or, l'intelligence artificielle semble introduire de nouvelles normes. La vitesse de transmission des ordres s'approche sensiblement de la vitesse de la lumière. Si des ordinateurs étaient capables de suivre la situation tactique, de l'interpréter et d'envoyer des instructions vers des machines automatisées pour agir de manière optimale, ils accompliraient les deux dernières fonctions de la boucle OODA, soit la décision et l'action, dans un temps bien plus court que tout autre système structuré autour des hommes. Le détenteur d'un tel système disposerait d'un avantage comparatif certain par rapport à un ennemi traditionnel. Le niveau de performance de l'intelligence artificielle et des systèmes qu'elle anime serait par ailleurs constant dans le temps car il ne serait pas fragilisé par la déconcentration, la fatigue ou le stress que les hommes peuvent ressentir.

Envisager d'automatiser complètement un grand nombre de systèmes pour des raisons opérationnelles serait-il raisonnable ? En réalité, la diffusion de l'intelligence artificielle et de l'automatisation sur le champ de bataille ne serait pas une initiative si audacieuse qu'on peut le penser. Des systèmes d'arme sont déjà mis en œuvre, qui réduisent la place de l'homme selon les circonstances. Ainsi, le système d'armes naval *Aegis*, introduit dans les années 1980 pour défendre la flotte américaine contre les attaques d'avions ou de missiles, comprend quatre modes : le « semi-automatique »,

dans lequel l'homme s'appuie sur le système pour décider lui-même quand tirer et quelles cibles viser ; l'« automatique spécial », pour lequel les opérateurs humains définissent les priorités, comme le type de cibles à abattre en urgence (par exemple les missiles d'abord, puis les bombardiers, puis les avions de chasse), mais en laissant le système agir par lui-même ; l'« automatique », où les données remontent vers les décideurs pour les informer, mais avec un système qui travaille seul ; et le mode « *Casualty* » dans lequel le système choisit les tâches qui lui semblent les meilleures pour assurer la survie du bâtiment[81]. Le développement des missiles hypersoniques ne ferait que renforcer le besoin de ce type de systèmes comportant une grande part d'automatisation, compte tenu des vitesses d'approche de ce type de munitions et du temps très réduit pour réagir. L'IA, en calculant les meilleures géométries d'interception et en sélectionnant certains postes de tir plutôt que d'autres, pourrait se révéler décisive pour contrer ce type d'attaque.

On conçoit aisément l'intérêt de l'automatisation dans certains milieux artificiels, comme celui du spectre électromagnétique pour la guerre électronique ou de l'espace cyber pour la guerre informatique. Le *Cyber Grand Challenge 2016* organisé par la DARPA a montré qu'il était déjà possible de détecter automatiquement certaines vulnérabilités dans les logiciels et réseaux adverses tout en améliorant la protection de ses propres systèmes[82]. Mais il est possible d'aller encore plus loin. Le couple IA/automatisation pourrait donner un avantage notable sur le champ de bataille si des unités de robots ou de plateformes distribuées agissaient de manière concertée dans l'espace et le temps en suivant les ordres d'une intelligence artificielle centralisée pour accomplir la manœuvre la plus adaptée. Leurs trajectoires, leurs tirs seraient déterminés en fonction des renseignements mis à disposition des logiciels et de l'expérience tirée de cas similaires dans le passé. Si une position devait par exemple être prise, la succession ou la synchronisation des attaques des robots seraient savamment orchestrées par les logiciels de l'IA pour feindre des attaques, user les ressources des défenseurs ou porter le coup de grâce. Des armes à énergie dirigée pourraient être activées, frappant régulièrement leur cible avec une précision encore jamais atteinte. Par ailleurs, l'homme n'étant plus en première ligne, la conception des robots pourrait être radicalement modifiée. La vitesse et la manœuvrabilité pour échapper aux tirs adverses pourraient être privilégiées là où le blindage et les lourdes contre-mesures emportent parfois l'adhésion aujourd'hui.

81. P. W. Singer, *Wired for War*, New York, Penguin Books, 2010, p. 124.
82. T. Berthier, « Les apports de l'intelligence artificielle en cybersécurité et cyberdéfense », *op. cit.*, p. 39.

Certains experts accompagnent ces réflexions par de nouveaux concepts et tentent de populariser leurs thèses avec de nouveaux slogans, comme « la guerre à la vitesse de la lumière » imaginé par Wang Weixing, directeur de recherche militaire dans l'Armée populaire de libération chinoise :

> « Le combat sans hommes est en train d'émerger progressivement comme le futur de la guerre. Même si la plupart des gens ont la tête dans le sable en essayant de réduire les écarts dans le domaine des armes traditionnelles avec les puissances militaires mondiales, la guerre à la vitesse de la lumière guidée par la technologie est sur le point d'occuper la place centrale.[83] »

Dans le même esprit, l'*Hyperwar* est théorisée par le général John Allen du corps des Marines comme « un type de conflit où le processus humain de décision est pratiquement complètement absent de la boucle OODA de l'IA. En conséquence, le temps correspondant à un cycle OODA sera réduit à des réponses quasi instantanées », et ajoute-t-il, « les implications de ces développements sont nombreuses et changent les règles du jeu[84] ».

Il est également possible d'imaginer un emploi décentralisé de l'intelligence artificielle avec des systèmes d'arme automatisés radicalement différents de ceux conçus aujourd'hui. Le *swarming* (ou « manœuvre en essaim ») incarne une autre révolution qui pourrait frapper le champ de bataille[85]. L'essaim est constitué d'une flotte de robots, généralement similaires et de petite taille, qui suivent des règles simples et interagissent entre eux à l'aide de logiciels. Aucune autorité centrale ne les guide mais l'ensemble de leurs actions non linéaires engendre un comportement global cohérent, *a priori* ignoré par chaque élément. Une IA peut rendre plus efficace ou robuste un essaim face à des menaces pour adapter ses règles de base et son comportement général. Leur association les rend redoutable.

La grande qualité d'un essaim est de pouvoir saturer un adversaire. S'il est constitué de dizaines, voire de centaines de composants pouvant causer des dommages, il est difficile de s'en défendre sans devoir tous les éliminer. De telles formations pourraient-elles avoir raison des systèmes d'arme complexe actuels, conçus pour prévaloir sur des systèmes d'arme du même

83. E. Feng et C. Clover, « Drone Swarms vs. Conventional Arms: China's Military Debate », *Financial Times*, 24 août 2017, disponible sur : www.ft.com.
84. J. R. Allen et A. Husain, « *On HyperWar* », *Proceedings Magazine*, vol. 143, n° 373, juillet 2017, disponible sur : fortunascorner.com.
85. J. Arquilla et D. Ronfeldt, *Swarming and the Future of Conflict*, Santa Monica, RAND Corporation, 2000, p. 102.

type, mais qui ne sont produits qu'en faible nombre compte tenu de leur coût ? Si les essaims possèdent leurs propres limites, comme de faibles rayons d'action par exemple par rapport à ceux des avions de chasse ou des navires les plus modernes dont les capacités d'emport sont bien plus élevées, le fait qu'ils puissent endommager des pièces essentielles du dispositif adverse et qu'ils augmentent sensiblement les risques d'attrition sans être sensible aux pertes ouvre la porte à la réflexion sur le développement de solutions alternatives.

La diffusion de l'intelligence artificielle a ainsi le mérite de redonner une nouvelle vigueur au débat quantité contre qualité qui a été tranché en Occident en faveur du second terme. L'IA pourrait réintroduire de la qualité à faible coût dans la quantité. De la même manière qu'elle pourrait chasser du marché du travail de nombreux employés, l'IA pourrait congédier à terme des combattants ou des systèmes d'arme complexes. Des robots simples mais nombreux s'imposeraient de plus en plus, animés par les algorithmes et processeurs à l'œuvre dans les boucles de décision. À terme, la guerre s'automatiserait de façon exponentielle.

Quand l'homme domine la machine : l'apport de l'humanisme militaire

Si les évolutions de l'intelligence artificielle faible semblent prometteuses à moyen terme, de nombreuses voix appellent néanmoins à ne pas en surestimer le potentiel et à mieux prendre en compte les limites technologiques, le risque d'une perte de contrôle et l'existence de contre-stratégies efficaces permettant d'en réduire l'impact. Prenant en compte ces points d'attention, ces critiques du « tout technologique » en appellent à un « humanisme militaire » qui conserve l'homme au cœur des processus de décision, donnant à la machine le rôle d'équipier fidèle.

Les limites technologiques

Une première objection au développement incontrôlé de l'automatisation est que toute technologie suscite ses propres limites, qu'il convient d'identifier afin de mieux s'en prémunir. Rappelons d'abord que le fonctionnement nominal des systèmes ne va pas de soi. Les informaticiens doivent faire face à de nombreux défis pour faire fonctionner les réseaux, comme la lutte contre les cyberattaques. Et de nouvelles frictions apparaissent au sein de ces systèmes à mesure qu'augmente le nombre d'acteurs concernés, d'interactions potentielles et de sources de données. Les opérateurs devront également faire face aux problèmes de stockage de données alors même que la

performance des intelligences artificielles dépend du volume de ces dernières et de leur accès.

Des progrès restent à accomplir pour améliorer les performances des algorithmes. Deux expériences dans le domaine de la reconnaissance d'image sont souvent mises en avant pour illustrer leurs fragilités. Dans la première, un autocollant est appliqué sur un panneau « STOP ». Le réseau neuronal est abusé par la variation de l'image qu'il doit analyser. Il discerne mal le changement et interprète le panneau d'arrêt comme un panneau de limitation de vitesse. Dans la seconde expérience, une intelligence artificielle qui parvient à identifier l'image d'un panda dans 57,7 % des cas peut reconnaître un gibbon sur la même photo avec une certitude de 99,3 % si la valeur des pixels de l'image varie de 0,04 %[86]. Les résultats ne sont donc pas complètement fiables. Des adversaires peuvent faire échouer la reconnaissance de certains objectifs en jouant sur la manière dont les logiciels codent les images.

De même, l'évolution du contexte opérationnel peut provoquer l'obsolescence des lois d'apprentissage des algorithmes. L'exemple de l'élaboration des *Improvised Explosive Devices* (IED) en Irak et de leur complexification au cours du temps est de ce point de vue très instructif. Les insurgés en Irak avaient imaginé plus de 90 procédés différents pour déclencher leurs IED en 2007. Leur but était de tromper à chaque fois les contre-mesures américaines. Quand l'*US Army* introduisit par exemple des robots pour détruire ces IED, les activistes irakiens placèrent des petits murs de ciment ou de détritus autour de l'engin explosif pour gêner la progression des automates. Certains les placèrent même en hauteur[87].

La dialectique de l'épée et du bouclier s'appliquera donc aussi à l'intelligence artificielle. Les systèmes d'apprentissage sont aujourd'hui bien adaptés pour répondre à des tâches ou des questions précises. Ils jouent très bien aux échecs ou au go, mais ne savent pas jouer aux échecs sur un échiquier différent car personne ne l'a imaginé. Comment les pièces devraient-elles être placées, combien de temps la reprogrammation durerait-elle pour tenir compte des dimensions plus grandes du « terrain de jeu » ? L'adversaire tentera d'emmener l'IA sur des terrains où elle peine à fonctionner. Les algorithmes devront être suffisamment agiles dans l'avenir pour s'adapter à des situations ouvertes, où les règles du jeu, les acteurs ou l'environnement peuvent se transformer brutalement.

86. R. Richbourg, « It's Either a Panda or A Gibbon: AI Winters and the Limits of Deep Learning », *War on the Rocks*, 10 mai 2018, disponible sur : warontherocks.com.
87. P. W. Singer, *Wired for War, op. cit.*, p. 218-219.

La qualité des algorithmes n'est pas la seule limite au développement de l'intelligence artificielle sur le champ de bataille. Des biais cognitifs dans la sélection des données peuvent aussi altérer la pertinence des réponses données par l'intelligence artificielle. Si les manifestations sexistes ou racistes ont été stigmatisées à l'occasion d'expérimentations malheureuses, force est de constater qu'elles sont d'abord la conséquence de préjugés ou du sens commun[88]. Des chercheurs ont ainsi employé le logiciel d'apprentissage non supervisé *GloVeen* en l'entraînant avec 840 milliards d'exemples piochés sur internet pour découvrir les associations que les utilisateurs en ligne faisaient entre certains termes[89]. Des mots tels que « féminin » ou « femme » étaient souvent liés avec des professions d'art tandis que les termes « masculin » et « homme » étaient conjugués aux métiers scientifiques. Une intelligence artificielle fera automatiquement les mêmes rapprochements si les logiciels sont conçus pour les valoriser, si les bases de données sont réduites inconsciemment pour satisfaire nos représentations par rapport au genre.

D'une manière générale, une intelligence artificielle apprend comme un jeune enfant : elle reproduit les comportements présents dans son environnement et dépend beaucoup du type d'éducation qu'elle reçoit. Dans le domaine militaire, ces biais pourraient se traduire par la valorisation de certains modes d'action par rapport à d'autres, avec la conception d'algorithmes par des composantes d'armée particulières sélectionnant les solutions mettant le plus en valeur leurs propres organisations. Cela pourrait aussi se traduire, dans un contexte de contre-insurrection, par l'entretien d'une méfiance exacerbée contre certaines parties de la population traditionnellement hostiles à notre présence.

La perte de contrôle

Un autre défi que pose l'intelligence artificielle est l'impossibilité de suivre en temps réel les raisonnements que la machine adopte pour trouver la solution. Les logiciels traduisent dans leur propre langage les problèmes qui leur sont posés et proposent des solutions en suivant différentes phases logiques qui ne peuvent être contrôlées directement. De nombreuses pages de calcul doivent être décodées pour apprécier la justesse et le raffinement de la méthode. Le principe de boîte noire s'impose donc pour l'instant. Si une machine propose

88. Microsoft a lancé en 2016 une IA appelée « Tay », censée figurer une adolescente s'exprimant sur Twitter. Les échanges qu'elle entretint pendant quelques heures avec des êtres humains, souvent de mauvaises fois, la transformèrent en une plateforme prônant le racisme et le négationnisme. Tay fut débranchée très rapidement. Lire à ce sujet : M. Tual, « Quand l'intelligence artificielle reproduit le sexisme et le racisme des humains », *Le Monde*, 15 avril 2017.
89. R. Bhatia, « Biaised AI: Princeton Study Indicates Race and Gender Bias Has Crept into Machine Learning Algorithms », *Analytics India Magazine*, 24 avril 2017.

une solution originale qui doit être appliquée dans des temps relativement courts, l'emploi de l'intelligence artificielle peut se révéler désastreux en créant le doute, en nourrissant des interrogations et en causant une perte de temps. Ces interrogations seraient amplifiées dans le cadre d'une coalition, où le détenteur de l'autorité pourrait imposer à ses alliés certains modes d'action, en se retranchant derrière les conclusions des algorithmes. Il serait sans aucun doute très contesté si ses ordres mécontentaient ses partenaires et s'il ne pouvait justifier rapidement ses orientations.

Tandis que le décideur doit conserver une distance par rapport aux orientations qui lui sont suggérées, l'humain croit souvent que les machines lui sont supérieures. Et en cas de défaillance de la machine, l'accident est alors d'autant plus probable, comme lorsque le conducteur enthousiaste d'un véhicule autonome perdit la vie en s'encastrant avec sa voiture dans un tracteur. Il faisait trop confiance au pilote automatique qui, *a priori*, ne sut pas faire la différence entre l'éclat du ciel et le blanc de la remorque du tracteur[90]. Contrairement aux avertissements du constructeur Tesla, il ne gardait pas les mains sur le volant par sécurité. Un système mis en œuvre par des opérateurs mal entraînés ou peu expérimentés, possédant dans sa gamme des modes automatisés, a de fortes chances d'être employé de manière complètement automatisée[91].

Les équipes en charge des batteries de missiles sol-air *Patriot* opéraient par exemple en mode automatique lors de l'invasion de l'Irak en 2003, convaincus de la supériorité de leur système à la suite des résultats obtenus en 1991 lors de la première guerre du Golfe, qui étaient jugés encourageants. Or, les logiciels employés étaient dérivés du système antibalistique *Safeguard* qui travaillait en atmosphère haute, dans un milieu où la circulation aérienne était très réduite. Ces logiciels étaient conçus pour tirer dans la plupart des cas. Comme les batteries surveillaient l'atmosphère basse en 2003, où la fréquence de passage d'avions en transit était beaucoup plus élevée, la logique programmatique agressive fut fatale à un équipage de *Tornado* britannique. L'ordre de tir fut donné automatiquement par la machine quand certains critères furent remplis, sans qu'aucun opérateur n'intervienne[92].

Tirant l'expérience de cet accident, le mode de tir automatique fut déconnecté pour empêcher d'autres drames. Seul le mode d'engagement

90. S. J. Freedberg Jr., « Artificial Stupidity: Fumbling the Handoff from AI to Human Control », *Breaking Defense*, juin 2017, disponible sur : breakingdefense.com.
91. J. K. Hawley, « Patriot Wars: Automation and the Patriot Air and Defense Missile System », *Center for a New American Security*, janvier 2017.
92. S. J. Freedberg Jr., « Artificial Stupidity: Fumbling the Handoff from AI to Human Control », *op. cit*.

était conservé dans cet état, ce qui permettait de suivre la trace de cibles potentielles, de gagner du temps pour analyser la situation avant de décider du tir éventuel. Mais les opérateurs comprenaient mal les connections entre les différents modes. Quand un capteur rapporta qu'un missile *Scud* était peut-être en train de converger vers les positions américaines, le responsable tactique d'une batterie ordonna de préparer les lanceurs, c'est-à-dire de faire en sorte qu'ils soient en état de tirer s'il le décidait. Les opérateurs ne saisirent pas l'esprit de l'ordre et reconnectèrent l'ordinateur de contrôle du tir, qui était resté en mode automatique, avec les autres éléments du système. Une salve de missiles s'élança alors immédiatement dans le ciel à la grande surprise du chef tactique. Un F/A-18 de l'*US Navy* fut abattu et son pilote tué[93]. L'automatisation s'avérait plus meurtrière que l'armée de l'Air irakienne.

Ces exemples montrent que la gestion des opérations avec des systèmes automatisés peut très rapidement échapper à ses responsables. Plus l'automatisation des systèmes augmente, plus l'expertise des hommes est nécessaire pour bien comprendre les implications des options choisies, et faire face à un éventuel dysfonctionnement. Une intelligence artificielle orientera et guidera à terme une manœuvre selon sa propre logique, qui peut ne pas convenir aux chefs militaires.

Des contre-stratégies efficaces

Employer l'intelligence artificielle impose d'être vigilant face à ses carences technologiques et ses fonctionnements intrinsèques mais aussi face aux possibilités de son contournement par des contre-stratégies efficaces qui ne passent pas forcément par davantage de technologie. Lucides face au nouveau défi que pose la TOS, les observateurs russes explorent ainsi de nombreuses voies pour la mettre en échec. Ils sont conscients des limites de leurs moyens et savent qu'ils ne peuvent fournir des efforts sur une échelle comparable aux Américains. Aussi, le recours potentiel aux armes nucléaires stratégiques et tactiques demeure l'option préférentielle face aux agressions directes contre la Russie. Par l'ampleur des dommages potentiels causés, l'atome continue de balayer tous les avantages conventionnels que peuvent offrir les nouvelles technologies, dont l'intelligence artificielle[94].

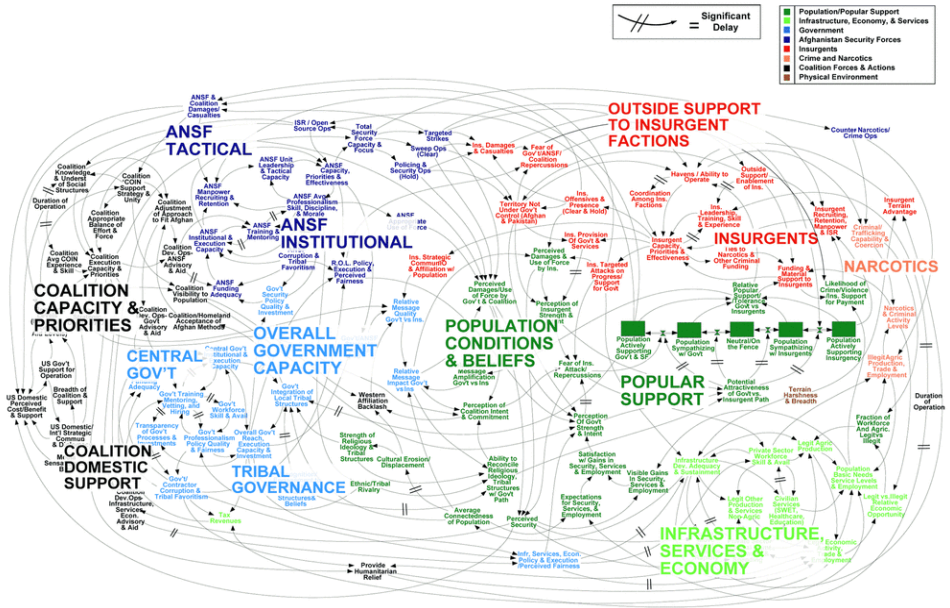
L'autre stratégie envisagée pour contrer la TOS est de se concentrer sur le développement des technologies qui pourraient le mieux concurrencer

93. J. K. Hawley, « Patriot Wars: Automation and the Patriot Air and Defense Missile System », *op. cit.*
94. V. Kashin et M. Raska, « Countering the U.S. Third Offset Strategy: Russian Perspectives, Responses and Challenges », S. Rajaratnam Scool of International Studies, Policy Report, janvier 2017, p. 14.

les Américains. L'intelligence artificielle elle-même en est bien sûr une[95]. Elle pourrait doper les performances des armes à énergie dirigée, des canons à propulsion électrique, des plateformes hypersoniques ou des drones sous-marins. Par ailleurs, le mouvement initié par les adversaires des forces occidentales pour faire face à la deuxième stratégie de compensation va se poursuivre. Ces opposants sont parvenus à renouveler progressivement à limiter leur infériorité initiale. Leurs contre-stratégies ont généralement évolué vers trois directions.

La première est celle de la guerre irrégulière. Les insurgés ont su intégrer les avancées technologiques diffusées à grande échelle pour améliorer leurs capacités dans le domaine de l'information (propagande et échanges d'information sur internet, emploi de téléphones portables sur le champ de bataille, etc.). Ils emploieront sûrement l'intelligence artificielle au travers de simples applications civiles (commerciales), mais qui devraient être suffisantes pour améliorer leurs performances. En outre, la supériorité informationnelle des armées occidentales s'est heurtée à la complexité des sociétés dans lesquelles se déroulent ces conflits. Le « terrain humain » est souvent très complexe et difficile à modéliser. La tentative de l'état-major du général McChrystal en 2009 de description des processus à l'œuvre dans l'insurrection afghane est de ce point de vue révélatrice.

La guerre d'Afghanistan vue par le général McChrystal (2009)



Source : consulting, Dynamic Planning for COIN in Afghanistan, 2009[96].

95. *Ibid.*, p. 16.
96. « Dynamic Planning for COIN in Afghanistan », *PA consulting*, 2009, p. 22, disponible sur : www.oss.net.

La diffusion de ce schéma en 2009 répondait au souhait du général américain de montrer aux responsables politiques que la pacification de l'Afghanistan serait longue et nécessiterait beaucoup d'investissement et d'efforts. Pour autant, il « simplifie » une situation peu évidente à appréhender et montre les obstacles que devraient surmonter les ingénieurs informaticiens pour définir des algorithmes utiles. Si une meilleure maîtrise technologique et managériale de l'intelligence artificielle peut laisser augurer des résultats d'une qualité supérieure à ceux obtenus au Vietnam, choisir la vitesse comme fondement de sa stratégie peut s'avérer être une grave erreur. Ce type d'opérations prend place au sein de sociétés dont le rythme de fonctionnement ou d'évolution est d'un ordre complètement différent de celui de la vitesse des électrons. Dans ce cadre, une bonne exploitation des données dépend autant des considérations politiques et des contraintes locales que de leur intérêt militaire. La supériorité militaire occidentale, soutenue par l'intelligence artificielle, pourrait être défiée sérieusement dans un tel cadre.

La deuxième contre-stratégie a consisté à faire des efforts dans des domaines où les armées occidentales investissent peu, qu'elles délaissent ou que leur doctrine peine à aborder de manière satisfaisante. Il s'agit de contourner leurs points forts pour s'attaquer à leurs points faibles, d'être capable de combattre en même temps de manière régulière et irrégulière, d'étendre le champ de bataille aux domaines médiatique, économique, diplomatique et même culturel par des actions de violence. Il est probable que les opposants du camp occidental poursuivront dans la voie de ce que certains experts qualifient de « stratégies hybrides[97] ». Il s'agira alors d'accroître la complexité d'un théâtre et la difficulté à le modéliser en multipliant les acteurs avec des logiques propres, en augmentant les catégories de combattants avec l'emploi de supplétifs, de milices locales, voire de mercenaires. Les éventuelles capacités de prédiction des intelligences artificielles seront ainsi très diminuées. De telles stratégies pourraient aussi chercher à systématiser l'emploi de systèmes à usage dual, ou même, dans le militaire, à charge conventionnelle ou NRBC, ce qui compliquera singulièrement les calculs des stratèges et des logiciels. D'une manière générale, tous les modes d'action pouvant ajouter de la complexité seront probablement favorisés à l'avenir, notamment par leur propension à déjouer les prédictions établies par l'intelligence artificielle.

La troisième catégorie de contre-stratégie consiste au contraire, à rivaliser avec les Occidentaux *via* la mise en place de nouveaux systèmes d'arme surface-air ou surface-mer performants, destinés à contester leur

97. É. Tenenbaum, « Le piège de la guerre hybride », *Focus stratégique*, n° 63, Ifri, octobre 2015, disponible sur : www.ifri.org.

supériorité dans les espaces communs[98]. Des investissements significatifs ont été également réalisés pour produire une nouvelle génération d'armements terrestres. La valorisation de la guerre électronique ou de la cyberguerre a pour objectif de détecter et détruire les nœuds de contrôle et de commandement. Le résultat est aujourd'hui la création de nouvelles « forteresses » défendues par des systèmes sophistiqués sol-air et surface-mer qui empêchent l'accès à certaines zones par les forces occidentales et compliquent leur projection[99]. Cette stratégie symétrique sera peut-être celle que l'intelligence artificielle contrera le plus aisément car elle pourra comprendre en partie comment ces systèmes fonctionnent, analyser leurs performances et aider à concevoir des profils d'attaque pour les mettre en échec grâce au recueil de renseignement ou aux enseignements retenus lors de l'emploi futur de ces systèmes d'arme. Sur ce point au moins, l'avance technologique pourrait rester dans le camp occidental dans un premier temps.

L'humanisme militaire

Les doutes sur la fiabilité et la supériorité de l'intelligence artificielle s'ajoutent au scepticisme de nombreux observateurs quant aux apports réels des avancées informatiques dans le domaine politico-militaire, éthique ou culturel.

Les progrès de l'intelligence artificielle peuvent peut-être aider à triompher dans des affrontements tactiques, voire à gagner des batailles dans l'avenir, mais ces perfectionnements seront insuffisants pour remporter la guerre. Comme le note Clausewitz, la guerre s'inscrit d'abord dans un environnement politique. La victoire sur le champ de bataille n'a d'intérêt que si elle modifie le rapport de force politique en sa faveur. La victoire française de la Moskova en 1812 aux portes de Moscou ne modifie en rien la résolution du tsar Alexandre I[er] qui est décidé à lutter par tous les moyens qui lui restent pour chasser Napoléon de Russie. Or les intelligences artificielles faibles seront incapables dans un futur proche de saisir le contexte dans lesquels s'inscrivent leurs décisions ou leurs actions. Elles ne peuvent approcher tout ce que nos actions comprennent d'ambiguïté, de subjectivité, au cœur des interactions entre êtres humains. La politique reste le domaine de l'homme, qui diffère sensiblement du domaine mathématique des intelligences artificielles.

98. C. Brustlein, É. de Durand et É. Tenenbaum, *La suprématie aérienne en péril : menaces et contre-stratégies à l'horizon 2030*, Paris, La Documentation française, 2014, p. 256.
99. J.-C. Noël, « A2/AD », cité *in* B. Durieux, J.-B. Jeangène-Vilmer et F. Ramel, *Dictionnaire de la guerre et la paix*, Paris, PUF, 2017.

Au point de vue éthique, les arguments avancés contre le développement de l'IA reposent sur les principes simples qu'aucun être humain ne doit être tué par une machine autonome ou que les responsabilités doivent être clairement établies dans les chaînes de tir. Transiger avec ces règles revient à ouvrir la porte à tous les abus et excès, ce qui est inacceptable. Une IA pourrait par exemple suggérer à un responsable militaire d'employer telle unité dans un rôle de diversion tandis que telle autre effectuerait l'assaut principal, en fonction des informations éparses qu'elle détiendrait, comme l'état physique des soldats qui les composent. La machine déciderait alors du destin des hommes, à la place de l'officier en charge de la manœuvre. Les pertes seraient justifiées par un algorithme plutôt que par la décision d'un homme.

L'homme demeure en outre le seul capable de juger du caractère moral d'une action, dans le respect des valeurs qu'il défend, notamment dans des environnements complexes où civils et militaires évoluent en étant imbriqués[100]. La traduction en langage informatique d'un code éthique qui serait respecté par l'intelligence artificielle ou des systèmes d'armes automatisés suscite toujours un débat quant à sa faisabilité et son intérêt[101]. La littérature sur le sujet de l'éthique et de l'automatisation des armes est imposante et le contenu des arguments des experts suffisamment connus et répétés pour ne pas les exposer une fois de plus ici[102].

Enfin, d'un point de vue culturel, l'introduction de systèmes informatisés est très mal acceptée par des militaires dont l'*éthos* est d'abord fondé sur la possibilité de donner et de recevoir la mort. Le guerrier pourrait tomber de son piédestal. Le soldat doit en effet posséder ou acquérir par l'entraînement les ressources nécessaires pour affronter et dominer cet horizon tragique de la mort. La grandeur du métier de militaire est de pouvoir faire face aux tensions et aux risques, de maîtriser ses gestes et ses peurs, et d'accepter de se dépasser jusqu'au sacrifice si besoin est. Choisir des robots pour combattre en première ligne est une remise en cause radicale du monopole de l'homme au cœur du champ de bataille et une atteinte potentielle aux vertus qui fondent les armées depuis leur création.

L'ensemble des experts, commentateurs, professionnels ou simples citoyens qui contestent l'essor incontrôlé de l'intelligence artificielle dans

100. On notera néanmoins que les « Lawbots », algorithmes accomplissant des tâches judiciaires mineures mais répétitives, sont l'un des plus grands chantiers de l'IA. Leur assistance juridique aux armées pourrait sensiblement augmenter dans le futur.
101. B. Erbland, *Robots tueurs : que seront les soldats de demain ?*, Paris, Armand Colin, 2018.
102. On peut commencer pour avoir une vue générale avec F. Allhoff (dir.), *Routledge Handbook of Ethics and War: Just War Theory in the 21st Century*, Londres, Routledge, 2013.

les affaires stratégiques participe, parfois pour des motifs très différents, à un vaste mouvement qu'on pourrait qualifier d'humanisme militaire. Ce mouvement ne s'appuie pas sur un manifeste ou des textes fondateurs, mais regroupe simplement des hommes qui pensent que la guerre est une chose trop sérieuse pour être laissée aux algorithmes. Le sort des entités humaines constitue la finalité de la guerre et l'homme en est la pierre angulaire. C'est lui qui la déclenche, qui la mène, qui y combat, qui y meurt parfois, et enfin, qui la termine. Le respect de sa dignité doit y être assuré. C'est lui qui doit imposer sa volonté à son adversaire et sa loi aux systèmes d'armes ou aux systèmes informatisés qui le soutiennent, et non l'inverse.

L'équipier fidèle

L'humanisme militaire n'appelle pas pour autant à rejeter tous les artifices technologiques. La machine doit simplement assister l'homme et l'aider à accomplir certaines tâches avec plus d'intensité, plus de précision, plus d'efficacité, mais toujours sous son contrôle, sans jamais le dépasser. Le modèle de « l'équipier fidèle » (*loyal wingman*) est de ce point de vue assez satisfaisant. Un robot est étroitement associé à un homme en charge d'un système d'arme (comme un avion de chasse, un blindé ou même un navire). Ce robot a une autonomie cognitive limitée. Il ne pense pas par lui-même, mais répond aux intentions de son « maître ». Il est par exemple doté d'une réserve de munitions, peut mettre en action des capteurs supplémentaires, peut éventuellement fournir de l'énergie au système d'arme dominant pour qu'il accomplisse sa mission plus longtemps. Il amplifie d'une manière générale les ressources dont dispose le guerrier qu'il accompagne.

Utiliser à bon escient cet équipier fidèle nécessitera de l'entraînement. Il faudra bien connaître ses capacités, savoir l'appeler au bon moment. L'intelligence artificielle intégrée dans le système de l'équipier pourra jouer un rôle important pour faciliter cette relation particulière. Elle pourra apprendre comment se comporte son leader, anticiper ses initiatives, ses réactions. Elle pourra le suppléer pour surveiller une partie du ciel, du terrain ou de la mer, l'alerter en cas de danger impromptu ou mal pris en compte, lui signaler qu'une cible éventuelle est dans son domaine de tir.

Quelles que soient ses qualités, l'intelligence artificielle aura dans ce cadre un rôle en retrait par rapport à l'homme, qui serait donc acceptable. Le coût conceptuel et culturel sera, en définitive, limité par rapport aux pratiques actuelles, puisque la relation chef-subordonné structure les

armées[103]. Une telle solution offre enfin l'avantage de pouvoir être développée à brève échéance.

Une troisième voie : regrouper les robots en troupeau

L'opposition entre l'autonomisation à marche forcée du champ de bataille et l'humanisme militaire polarise un débat dont la seule issue semble la domination totale d'un modèle sur l'autre. Des solutions existent cependant pour faire cohabiter les deux visions, pourvu qu'on reprenne différemment les termes du débat.

La question de l'autonomie doit d'abord être relativisée. D'un point de vue théorique, l'autonomie absolue n'existe pas, que ce soit pour un soldat ou pour un système dépendant de logiciels. L'un et l'autre n'émergent pas du néant. Le premier est entraîné par d'autres hommes, suit des ordres et des procédures, et appartient à une organisation avec sa propre culture, tandis que le second est fabriqué par des ingénieurs qui, comme nous l'avons vu, possèdent leurs propres biais, leurs propres croyances et choisissent certaines options plutôt que d'autres pour écrire les lignes de programmation des algorithmes. Par ailleurs, les guerriers comme les robots sont des acteurs sociaux qui façonnent autant qu'ils subissent leur environnement. Ils doivent tenir compte des règles de communication collective pour interagir avec les autres acteurs. Ils doivent intégrer les valeurs prégnantes du groupe, mesurer les conséquences symboliques de leurs actes pour être efficaces. Autrement, le risque est grand que leurs interventions soient incompréhensibles pour les autres acteurs, par manque de cohérence avec la vision du monde de l'organisation. Un robot intégré dans les armées occidentales qui agirait actuellement sans souci des dommages collatéraux envers les civils ou sans prise en compte de paramètres éthiques serait vite retiré des unités de combat par exemple. Si leurs engagements provoquent des résultats inacceptables ou inintelligibles, ils cesseront d'être employés et leur entraînement, leurs algorithmes ou les processus de mise en œuvre seront complètement revus.

Contrôler sans dominer

Intégrer des systèmes autonomes dans un environnement où des humains agissent est l'une des tâches les plus complexes pour une intelligence artificielle. Le président Obama promulguait un nouveau règlement, en

103. D. Wassmuth et D. Blair, « Loyal Wingman, Flocking and Swarming: New Models of Distributed Airpower », *War on the Rocks*, 21 février 2018, disponible sur : warontherocks.com.

février 2012, qui ordonnait à la *Federal Aviation Administration* (FAA), direction en charge de la circulation aérienne aux États-Unis, de créer les conditions indispensables aux vols des drones dans l'espace aérien américain, déjà surchargé par les autres trafics[104]. L'idée était de profiter de l'avance américaine dans le domaine de l'automatisation aérienne pour la transformer en avantage économique et diffuser dans le monde un modèle de normes américaines. Initialement prévu pour fin 2015, le projet est toujours en cours et loin d'être achevé face aux difficultés posées par la cohabitation de systèmes habités et de systèmes autonomes[105]. Les ingénieurs de Google se heurtent également à de nombreuses difficultés pour mettre au point des voitures respectant scrupuleusement le Code de la route, tandis qu'elles évoluent sur des routes où les conducteurs humains s'affranchissent régulièrement des règles par inattention ou par choix. Enfin, l'exemple déjà cité des tirs intempestifs des missiles de batterie *Patriot* en 2003 confirme ces difficultés dans le domaine militaire.

Pourtant, il est possible que cette voie s'impose progressivement. Prenons une échelle de mesure de l'automatisation, où la note de 0 correspond à un système entièrement conçu pour l'homme et celle de 10 à celui qui est complètement automatisé. Le professeur d'aéronautique David A. Mindell montre que la note 5 correspondrait le mieux à la manière dont les projets aéronautiques et spatiaux qu'il a étudiés, comme le programme *Apollo*, ont été pensés et élaborés[106]. Alors que le pilotage des engins spatiaux qui se posèrent sur la Lune aurait pu être accompli de manière complètement automatique, les ingénieurs durent céder à de nombreuses pressions pour intégrer plusieurs manettes et commandes de vol, afin que l'équipage puisse prendre le contrôle des opérations dans certaines phases de vol comme l'alunissage[107]. De même, les robots *Rover* qui explorent la planète Mars peuvent être contrôlés depuis la Terre, et ce malgré les délais de communication d'une vingtaine de minutes entre notre astre et la planète rouge. Il aurait pu sembler pertinent de laisser le robot agir seul pour mieux faire face à des obstacles ou à des imprévus. Mais les scientifiques de la NASA ont estimé que le temps n'était pas le facteur décisif pour la réussite de la mission. Tant pis s'il a fallu quatre années sur Mars pour accomplir l'équivalent d'une semaine de travail d'un géologue sur Terre. En conservant la possibilité de lui donner des instructions, les

104. W. C. Bennett, « Unmanned at Any Speed: Bringing Drones into Our National Airspace », *Issues in Governance Studies*, Brookings Institute, n° 55, décembre 2012, disponible sur : www.brookings.edu.
105. R. Govan, « Former FAA Chief Counsel: Integration Pilot Program Strengthens U.S. Leadership in Drone », *Unmmanned Aerial Online*, 22 mai 2018, disponible sur : unmanned-aerial.com.
106. D. A. Mindell, « Driveless Cars and the Myths of Autonomy », *The Huffington Post*, 6 décembre 2017.
107. D. A. Mindell, *Digital Apollo: Human and Machine in Space Flight*, Cambridge, MIT Press, 2011.

scientifiques ont la sensation que le *Rover* est une partie d'eux-mêmes dématérialisée sur la planète rouge[108].

Cette règle du « 5 parfait », comme l'énonce David Mindell, montre que l'essentiel n'est pas que l'homme domine la boucle de décision ou qu'il soit constamment présent pour imposer sa volonté. À rebours, il ne peut se satisfaire d'être assujetti. Il doit donc être placé à l'intérieur de la boucle et être capable de rétroagir sur les décisions de la machine. Il doit avoir la possibilité de reprendre le contrôle du processus en cours quand il juge que l'intelligence artificielle lui a apporté les éléments qu'il souhaitait ou quand les enjeux sont importants.

L'ère des centaures

Le but pour les êtres humains doit donc être de privilégier une relation homme-machine harmonieuse, à la manière dont les joueurs d'échecs appelés « centaures » la pratiquent. À la manière de la figure mythologique mi-homme, mi-cheval, ils peuvent combiner le meilleur des ressources offertes par deux entités. Ces joueurs jouent à leur jeu préféré en « style libre ». Disposant d'un temps limité, ils sont autorisés pendant leurs parties à échanger avec des partenaires, à consulter des sources extérieures, à explorer des livres compilant les coups des maîtres, à utiliser des logiciels ou des moteurs de recherche fouillant dans des bibliothèques de parties passées. Si une intelligence artificielle peut leur proposer des options à chaque tour et les influencer fortement, ce sont les joueurs qui décident du mouvement de leurs pièces. Et cette association s'avère très fructueuse[109]. En 2005, deux amateurs d'échecs se servirent de 3 ordinateurs personnels pour gagner un tournoi dont le prix était de 20 000 dollars. Ils triomphèrent à cette occasion de grands-maîtres et même de super-ordinateurs[110]. Le secret de la victoire tenait dans l'excellente analyse de la personnalité et du style de jeu de leur adversaire. Les futurs vainqueurs sélectionnaient méthodiquement l'option de jeu offerte par les aides informatiques qui leur semblait la plus adaptée pour mettre en difficulté l'autre joueur. Ils ne tentèrent jamais de trouver le meilleur coup possible ou le chemin qui devait les emmener immanquablement vers la victoire.

108. D. A. Mindell, *Our Robots, Ourselves: Robotics and the Myths of Autonomy*, New York, Viking, 2015.
109. M. Cassidy, « Centaur Chess Shows Power of Teaming Human and Machine », *The Huffington Post*, 30 décembre 2014.
110. S. J. Freedberg Jr., « Breaking Defense, Centaur Army: Bob Work, Robotics and The Third Offset Strategy », *Breaking Defense*, 9 novembre 2015, disponible sur : breakingdefense.com.

Les centaures peuvent ainsi valoriser leur sens stratégique, en orientant la partie dans le sens qu'ils croient le plus adapté compte tenu de l'environnement, tout en bénéficiant de la puissance d'analyse méthodique de l'intelligence artificielle. Renoncer à un de ces deux atouts peut précipiter la défaite. Les grands maîtres sont d'ailleurs peu à l'aise dans ce style de jeu, car ils emploient mal les ordinateurs, estimant que leur connaissance du jeu est bien supérieure. On a cru en 1997, après la défaite du champion du monde Garry Kasparov face au programme *Deep Blue*, que l'histoire des joueurs d'échecs et des logiciels serait à sens unique. La pratique du style libre prouve l'inverse, en ouvrant d'incroyables possibilités.

Les robots domestiqués

Quelle serait la forme des nouveaux centaures sur le champ de bataille ? Il pourrait être les bergers de troupeaux constitués de robots spécialisés, les guides de nuées (*flocking*) où les oiseaux seraient remplacés par les automates. Le chef de tels dispositifs peut déléguer la réalisation de certaines tâches à ses fidèles accompagnateurs selon sa conception de la manœuvre ou, au contraire, exercer un contrôle direct et constant dessus dans certaines circonstances. Il peut imposer à chaque machine, comme le fait le leader avec son équipier fidèle, la surveillance d'une zone particulière d'espace aérien, de terrain ou de mer, et lui enjoindre de l'avertir si elle détecte une menace qui se rapproche. Mais il peut aussi diluer sa formation pour surveiller et contrôler un espace bien plus étendu que dans le cas précédent, attendant juste des comptes rendus réguliers. Si ces robots sont armés, il peut leur imposer certaines procédures avant de leur enjoindre de tirer ou, au contraire, les autoriser de manière préventive à détruire tout élément reconnu hostile sans avoir à renouveler son ordre. Il pourra ainsi se concentrer sur d'autres tâches comme le suivi attentif du déroulement de l'attaque d'un objectif assigné, maîtriser sa charge de travail dans des moments où les informations capitales se presseraient devant ses écrans et être plus créatif en cas d'imprévu. L'homme n'est plus dans la boucle mais sur la boucle. Il peut laisser faire tout en conservant la possibilité technique d'intervenir, voire d'interrompre certaines actions automatisées si elles ne lui conviennent pas. Il est responsable de la forme que prend son troupeau dans l'espace et de la manière dont il se comporte.

Le *flocking* n'est pas pour tout de suite. Des progrès sensibles dans le domaine de la fiabilité devront avoir été réalisés avant que certaines missions ne soient déléguées à l'intelligence artificielle. Les tirs fratricides des batteries *Patriot* en 2003 doivent à ce titre rester dans les mémoires. La délégation de l'autorité d'engagement devra avoir été finement étudiée

pour anticiper le plus de scénarios possible. Le chef de dispositif devra posséder une excellente compréhension des capacités des différents robots composant son troupeau, et faire un effort particulier pour saisir les modes de fonctionnement des algorithmes pour apprécier ce que l'intelligence artificielle peut lui offrir[111]. Certains pourront même argumenter que le contrôle de l'homme sur son troupeau sera illusoire car il ne pourra agir qu'en fonction des informations que l'intelligence artificielle aura sélectionnées pour lui. Mais la complémentarité homme-machine sera alors équilibrée et satisfaisante, puisque reposant sur l'exploitation des forces des uns et des autres.

Vers une utilisation sociale de l'intelligence artificielle

Cette recherche de l'harmonisation dans les relations homme-machine fait déjà l'objet d'études pour améliorer la performance des individus et des groupes. Des réflexions sont engagées dans le cadre de l'étude « *Man Machine Teaming* » chez des constructeurs aéronautiques comme Dassault Aviation pour déterminer la manière dont l'intelligence artificielle pourrait accompagner au mieux le pilote dans la gestion de son avion. Ainsi, le recueil de données sur l'état physique de l'équipage, sur sa concentration, sa fatigue, son état de stress pourrait permettre de mieux apprécier la disponibilité des aviateurs. En cas de doute sur l'intégrité de leurs capacités, des rappels pourraient être lancés si certaines actions vitales n'étaient pas effectuées. L'IA pourrait accomplir automatiquement des tâches précises dans des phases de vol critiques si elle considère que l'équipage est trop concentré sur d'autres aspects de la mission. Elle pourrait même ramener seule l'avion sur une base amie en suivant les contraintes d'une situation tactique si le pilote venait à être blessé, à perdre connaissance ou à être sérieusement diminué.

D'autres applications peuvent être imaginées pour mieux gérer les performances des soldats. Des projets existent déjà par exemple pour repérer les signes de stress post-traumatique. La thérapeute virtuelle Ellie, créée par l'Institute for Creative Technologies avec un financement de la DARPA, participe au traitement des vétérans atteints de syndrome de stress post-traumatique[112]. Personnifiée par un personnage féminin évoluant sur un écran placé face au patient, Ellie écoute sans juger, répond doucement, pose les bonnes questions mais n'offre aucun traitement. Elle utilise des

111. D. Wassmuth et D. Blair, « Loyal Wingman, Flocking and Swarming: New Models of Distributed Airpower », *op. cit.*

112. N. Jolly, « Meet Ellie: the Robot Therapist Treating Soldier with PTSD », *News.com.au*, 1er octobre 2016, disponible sur : www.news.com.au.

heures d'enregistrement pour identifier le langage corporel ou les gestes qui pourraient traduire la présence de vulnérabilité psychologique, comme le fait de se toucher directement la tête ou les mains.

L'intelligence artificielle pourrait également être employée dans une fonction préventive. Des robots pourraient être introduits au sein des unités pour engager des discussions régulières avec les soldats, simulant une intelligence empathique[113]. Ils contribueraient à déceler en amont certains traits de comportements, à les analyser, à les associer à un état psychologique. Ils pourraient suggérer des conduites préférentielles pour entretenir l'état moral et physique des soldats et pour prévenir certains risques. Lors d'affrontements, ils pourraient même stimuler l'ardeur des combattants ou calmer leurs craintes pour éviter une panique en énonçant les discours les plus adaptés.

Ces robots tiendraient-ils le rôle des officiers ? Lyautey, dans son article « le rôle social de l'officier », faisait remarquer que « les soldats aiment qui les aime[114] ». Un robot sympathique et compatissant pourrait peut-être devenir un rival menaçant pour l'autorité du commandement d'unité, si la valeur de celui-ci est faible. Mais dans la majorité des autres cas, l'intelligence artificielle fournirait d'abord une source supplémentaire de communication et de médiation entre les hommes et leur hiérarchie. Elle apporterait parfois des informations inédites au commandement. Peu de soldats professionnels admettront par exemple devant leurs frères d'armes qu'ils sont au bord de la dépression. Ils auraient l'impression de trahir le groupe ou leur engagement en admettant traverser des épreuves et ne plus se sentir à la hauteur. Ils ne le réaliseront peut-être pas eux-mêmes, étant éduqués pour repousser leurs limites. Une intelligence artificielle pourrait les mettre devant leurs propres contradictions.

La qualité de l'encadrement peut même ne pas être en cause. Le commandement peut être trop relâché à cause de la dispersion des troupes et des pertes subies, comme dans l'histoire réelle contée dans le livre *Black Hearts*[115]. De jeunes soldats américains de la *101e Airborne* ont vécu une vraie descente aux enfers pendant leur tour d'opérations en Irak, au milieu du triangle sunnite en 2005. Ils accusent alors des pertes nombreuses, avec des camarades parfois retrouvés massacrés et mutilés, ce qui accroît l'hostilité des parachutistes envers la population locale. L'encadrement est rapidement insuffisant et dépassé par la tâche, avec des troupes réparties sur un territoire trop grand, des cadres qui disparaissent et un état-major

113. Sur l'état de l'art des robots sociaux lire : L. Devilliers, *Des robots et des hommes*, Paris, Plon, 2017.
114. H. Lyautey, *Le rôle social de l'officier*, Paris, Broché, 2009 (1re éd. 1891).
115. J. Frederick, *Black Hearts: One Platoon's Descent into Madness in Iraq's Triangle of Death*, New York, Crown, 2010.

de division lointain et indifférent. La discipline se relâche lentement et les comportements se brutalisent jusqu'à l'irréparable. Isolés dans un poste en Irak, de jeunes soldats à l'équilibre psychologique précaire vont violer une jeune fille de 14 ans et la tuer avec sa famille. Affirmer qu'un robot social aurait pu les empêcher de passer à l'acte est certes très réducteur. Néanmoins, ces hommes sous pression auraient peut-être pu plus facilement se confier, parler de leur haine, apaiser leurs frustrations s'ils avaient été accompagnés par un robot social dans leur poste ou ailleurs. Savoir si ce dernier aurait pu proposer un discours salvateur et adapté aux différents protagonistes avant leur passage à l'acte est une autre histoire.

Confident ou commissaire politique ?

La route est cependant longue avant de voir de tels robots se multiplier dans les unités. Certains pourraient y voir des mouchards et seront peu désireux d'interagir ou de coopérer avec ces machines qui les trahiraient finalement en révélant leurs vulnérabilités à leurs chefs. Cette crainte nourrirait de la défiance et la cohésion de l'unité pourrait diminuer au lieu d'être consolidée. C'est pourquoi les règles devraient être claires dès l'introduction de ces robots, avec la mise à disposition de la hiérarchie d'un type réduit d'informations, acceptées par les chefs comme par leurs subordonnés. Des abus seraient-ils quand même à craindre ? La manière dont l'encadrement exploiterait certaines informations indues serait décisive et contribuerait, selon la bienveillance ou la répression affichée, à l'ambiance et aux performances de l'unité. Ainsi, la mise en place de robots sociaux n'abolirait pas les prérogatives de l'officier qui devrait toujours gérer les rapports humains dans son unité. Elle l'aiderait simplement à définir son action avec plus de connaissance.

L'acceptation de tels dispositifs dépendra sans aucun doute des cultures nationales et organisationnelles. Certaines unités, dont l'identité est construite sur un rapport particulier entre le chef et son subordonné, seront probablement rétives à voir un troisième acteur affecter cette relation. Les sensibilités nationales seront aussi déterminantes. Les robots font par exemple d'ores et déjà partie de la vie des Japonais, qui se sont accoutumés à évoluer avec eux. Ils les considèrent comme des amis, pensent même qu'ils possèdent parfois une âme et estiment en général que leur développement restera toujours sous le contrôle de leurs créateurs[116].

116. Z. Paré, *L'âge d'or de la robotique japonaise*, Paris, Les Belles Lettres, 2016 ; V. Pasquesoone et M. Gouesse, « Karyn Poupée : pour les Japonais, les robots ont une âme », *France Info*, 8 juin 2015, disponible sur : www.francetvinfo.fr.

Certaines expériences sur les théâtres de guerre d'Irak ou d'Afghanistan laissent penser que l'accoutumance pourrait également être rapide chez les soldats occidentaux. Les robots se sont multipliés dans l'armée de Terre américaine, en même temps que des comportements humains inattendus. Quand ces machines participent à des missions dangereuses, elles se voient attribuer des noms de célébrités, d'amies proches ou d'animaux domestiques. Des soldats ont donné leur médaille à des machines leur ayant sauvé la vie. Elles font partie de l'entourage proche. Michael Kolb, officier dans l'*US Army*, interrogea 746 hommes et femmes en opérations en 2011 pour mieux caractériser les relations homme-machine dans la guerre. Il constata que 80 % d'entre eux concédaient qu'ils aimaient ou appréciaient travailler avec des robots[117]. Il est donc possible à terme que les armées aient plus à craindre un surinvestissement des hommes envers les robots qu'une réelle désaffection. D'autres effets pervers devront alors être contrés, comme une implication affective déconcertante pouvant conduire un homme à se mettre en danger.

En définitive, les relations entre les hommes et les machines vont probablement évoluer sensiblement sous l'influence de paramètres technologiques, opérationnels mais également culturels. L'homme devrait conserver sa place centrale, mais concéder progressivement de plus en plus d'autonomie aux robots à mesure que leur fiabilité augmentera et que les militaires s'habitueront à travailler avec. L'intelligence artificielle pourrait même trouver une place particulière dans les relations entre homme. Mais dans ce domaine également, les robots devront d'abord faire la preuve de leur plus-value.

117. N. Subbaraman, « Soldiers vs Robots: Military Bots Get Awards, Nicknames … Funerals », *NBC News*, 28 septembre 2013, disponible sur : www.nbcnews.com.

En route vers une intelligence artificielle forte

Si la forme que prendra la relation homme-machine structurera en partie l'exploitation militaire de l'intelligence artificielle, la place du politique sera également essentielle. C'est lui qui décidera de l'importance à accorder à l'IA dans l'évolution du modèle de ses forces armées. Ses orientations stratégiques pourront influencer les doctrines militaires en la matière. Toutefois l'avènement d'une intelligence artificielle forte, la nature de la guerre pourrait évoluer d'une façon telle que la relation entre le politique et la guerre serait transformée, en gommant progressivement la place du militaire.

Miser sur l'intelligence artificielle

Le pari chinois : un projet structurant

La capacité à transformer du carburant en énergie mécanique a entraîné la motorisation générale des forces armées et la disparition, en l'espace de quelques décennies, du cheval qui était présent depuis trois millénaires dans les ordres de bataille. On conçoit aisément que si l'intelligence artificielle est un facilitateur comparable au moteur à explosion, la question de la priorité à accorder à cette technologie dans les futurs développements des systèmes de défense doit être posée.

Parmi l'ensemble des grandes puissances qui investissent dans l'intelligence artificielle, les États-Unis et la Chine se démarquent nettement par les efforts consentis. Les initiatives américaines prises dans le cadre de la *Third Offset Strategy* ont déjà été largement évoquées. Si les projets chinois restent plus discrets, il est en revanche certain que de nombreux responsables sont convaincus que l'IA sera disruptive et que sa maîtrise constituera la principale source de puissance militaire.

Depuis 30 ans, la Chine travaille à combler son retard technologique sur les États-Unis dans le domaine militaire. La prise de conscience de leur infériorité date de 1991, quand les armées de la coalition menées par les États-Unis écrasent en un temps très bref l'armée irakienne, alors considérée par certains comme « la quatrième armée du monde ». Militaires et politiques chinois réalisent avec effroi qu'ils ne disposent pas des équipements et des doctrines indispensables pour rivaliser avec la première puissance militaire mondiale. Dès 1993, la préparation en vue de

mener « des guerres locales à haute technologie » devient leur priorité[118]. Depuis, un lent grignotage de la domination américaine est entrepris, avec des résultats controversés puisque la qualité opérationnelle des unités chinoises n'a pu encore être évaluée dans des conditions de guerre réelle.

Or, l'émergence de l'intelligence artificielle permet d'entamer une nouvelle course contre les Américains en partant cette fois de la même ligne de départ. La victoire d'*AlphaGo* contre les meilleurs joueurs humains a été à ce titre une révélation pour les militaires chinois. Elle a prouvé tout le potentiel de l'intelligence artificielle, capable de mener seule des analyses complexes et d'établir des stratégies gagnantes[119]. Certes, les entreprises américaines dominent dans le domaine de la recherche, mais la Chine ne manque pas d'atouts. Outre la volonté politique, les liens étroits entre les secteurs privé et public en Chine pourraient être source de diffusion plus rapide des percées technologiques au profit de l'armée. Et les employés des firmes chinoises ne pourront faire pression sur leurs dirigeants pour limiter la coopération avec les militaires, comme l'ont fait les salariés américains de la firme Google pour manifester leur volonté de ne pas contribuer « au business de la guerre[120] ».

Alors qu'il apparaît que la Chine et les États-Unis seront probablement les deux plus grandes puissances militaires du XXIe siècle, ces dernières serviront de modèles ou de sources d'inspiration pour les autres nations. En investissant aujourd'hui massivement dans l'intelligence artificielle, elles ouvrent un chemin que d'autres puissances comme la France devront nécessairement suivre pour rester concurrentielles et fixent un modèle normatif pour les décennies à venir. Comme l'indique le général Liu Guozhi, directeur de la commission science et technologie de la commission centrale militaire du Parti communiste chinois, « qui ne se métamorphose pas sera disloqué[121] ». La guerre centrée sur l'information sera remplacée par la guerre centrée sur l'intelligence artificielle[122].

118. E. Puig, « L'arme du pouvoir et le pouvoir des armes : analyse des évolutions contemporaines de l'armée populaire de libération », *Revue française d'administration publique*, vol. 150, n° 2, 2014, p. 495-510.
119. E. B. Kania, « Battlefield Singularity: Artificial Intelligence, Military Revolution, and China's Future Military Power », Center for A New American Security, novembre 2017, p. 15.
120. X. Biseul, « Projet Maven : les salariés de Google refusent le "business de la guerre" », *Silicon*, 6 avril 2018, disponible sur : www.silicon.fr.
121. Cité *in* E. B. Kania, *op. cit.*, « Whoever Doesn't Disrupt Will Be Disrupted », p. 13.
122. E. B. Kania, « Battlefield Singularity: Artificial Intelligence, Military Revolution and China's Future Military Power », *op. cit.*

Les « hivers » de l'intelligence artificielle

Une condition est cependant nécessaire pour que l'intelligence artificielle libère son potentiel. Les avancées dans la recherche doivent se poursuivre et les performances technologiques doivent continuer à croître. Or, l'histoire de l'intelligence artificielle est une suite d'espoirs, d'avancées, mais aussi d'échecs. Il convient d'être mesuré lorsqu'on envisage l'essor de l'IA. Au moins deux « hivers » ont ponctué sa lente progression au tournant des années 1970 et à la fin des années 1980, car les chemins ont conduit à des impasses. La loi de Moore, qui n'est pas une loi physique mais un constat empirique, semble s'essouffler. Quant à la recherche sur l'informatique quantique, elle est prometteuse mais est loin d'être aboutie.

Les progrès récents ont beaucoup tenu à l'utilisation des réseaux de neurones. Le premier de ces réseaux est le perceptron, dont l'invention date de 1957[123]. Cinquante ans ont été nécessaires pour que cette machine soit améliorée, transformée, et serve de support dans des formes plus élaborées à l'apprentissage profond. Les avancées sont parfois longues à se concrétiser, dépendant du temps incompressible pour faire tomber les barrières théoriques ou technologiques. En outre, ces machines travaillant avec des réseaux de neurones ne peuvent effectuer aujourd'hui que certaines tâches.

D'autres découvertes seront nécessaires pour que les performances de l'intelligence artificielle se rapprochent de celles qu'annoncent ses thuriféraires. De nouvelles voies devront probablement être empruntées. Geoffrey Hinton, l'un des inventeurs de l'apprentissage profond, suggère ainsi que les chercheurs abandonnent les réseaux convolutifs, se débarrassent de la rétro-propagation et soutiennent … les réseaux de capsules (*capsule networks*[124]). Ce projet de recherche donnera-t-il des résultats rapidement ? Emprunte-t-il la bonne voie ? On ne le sait pas encore avec certitude. Le rythme des progrès en intelligence artificielle doit être évalué avec prudence.

Une technologie nouvelle pour faire face à des problèmes classiques

Le coût de l'introduction de l'intelligence artificielle dans les armées et des équipements associés pour l'exploiter avec succès est rarement évoqué car

123. N. J. Nilsson, *The Quest for Artificial Intelligence, op. cit.*, p. 92.
124. F. Cucci, « Deep Learning Is Not the AI Future », *KDnuggets*, 13 août 2017, disponible sur : www.kdnuggets.com ; J. Diaz, « "Réseau de neurones" : Geoffrey Hinton annonce un tournant fondamental », *ActuIA*, 2 novembre 2017, disponible sur : www.actuia.com.

il n'existe encore pas de modèle élaboré pour l'évaluer. Des investissements importants seront nécessaires, qui impliqueront des choix. Les coûts liés au stockage des données, à la sécurité des réseaux, au développement et à la mise à jour des logiciels très élaborés, au traitement des obsolescences pèseront sur les budgets. Le développement et la mise en place d'intelligences artificielles adaptées pour chaque niveau d'exécution et de commandement ne pourront être entrepris à budget constant qu'en sacrifiant d'autres équipements, ou contraindront d'équiper seulement quelques niveaux hiérarchiques. Le contenu des arsenaux devra être en partie revu pour acquérir différentes formes de robots.

Quelles priorités donner dans ce contexte ? Le chercheur américain Stephen Biddle soutenait lors des débats sur la RMA qu'une armée composée d'hommes bien entraînés mais équipés de matériels un peu plus anciens était préférable à une armée possédant des matériels de pointe mais moins bien préparée et entraînée[125]. La complexité du champ de bataille augmente certes à mesure que ses dimensions spatiales et temporelles s'accroissent. Mais les défis tactiques restent les mêmes depuis le début du XXe siècle. Si l'on se situe dans le milieu terrestre par exemple, on retrouvera des enjeux bien connus. En attaque, les unités doivent être capables de maîtriser le « système moderne de la tactique », qui incorpore la couverture, la dissimulation, la dispersion, la manœuvre indépendante des petites unités, les tirs de neutralisation, et l'intégration interarmes. En défense, les troupes doivent pouvoir utiliser avantageusement le terrain ou les positions en profondeur. Le commandement doit savoir contre-attaquer et employer ses réserves avec justesse[126]. Si les technologies changent, la forme du combat terrestre demeure. La modernisation des équipements est bien sûr utile et nécessaire, puisqu'elle amplifie l'écart qualitatif qui sépare deux armées. Mais elle doit être maîtrisée et ne pas se faire au détriment du volume d'autres capacités ou des doctrines éprouvées.

Investir de manière massive dans l'intelligence artificielle est un pari. Si les progrès espérés se matérialisent, le bond en avant sera patent. Les armées qui seront capables d'intégrer ces avancées domineront sans aucun doute les autres, en fonction des circonstances ou de la nature de la lutte. Pour autant, la recherche fondamentale et ses applications technologiques réclament du temps pour aboutir. Et en attendant, des processus classiques seront souvent suffisants pour résoudre les problèmes traditionnels de la guerre.

125. S. Biddle, W. P. Hinkle et M. P. Fisherkeller, « Skill and Technology in Modern Warfare », *Joint Force Quaterly*, été 1999, p. 18-25.
126. S. Biddle, *Military Power*, Princeton, Princeton University Press, 2004, p. 35-44.

Culture politique, doctrine militaire et intelligence artificielle

Un courant de l'histoire militaire américaine affirme que les régimes démocratiques sont les plus aptes à remporter les guerres – tout du moins les guerres majeures – car leurs citoyens acceptent plus naturellement les responsabilités et saisissent plus volontiers les initiatives. Ils combattent pour leur propre liberté et savent qu'ils risquent l'oppression en cas de défaite[127]. La culture politique aurait donc une influence directe sur la manière de lutter. L'emploi de l'intelligence artificielle pourrait-il aussi dépendre de la nature du régime politique qu'elle doit servir sur le champ de bataille ?

Le cas de l'Armée populaire de libération (APL) chinoise est de ce point de vue intéressant. Elle centralise d'une manière générale les décisions et tend à éviter la prise d'initiative par des acteurs les moins gradés. Son action est réglée et inspirée par les directives du Parti. L'adoption des technologies de communication modernes n'a pas profité aux échelons tactiques, mais a plutôt encouragé le micro-management par les échelons les plus élevés[128]. Il semblerait logique que cette tendance se poursuive pour maintenir la cohérence idéologique au sein de l'armée. L'étreinte de plus en plus resserrée de Xi Jinping sur l'APL pourrait même accentuer cette orientation. Les solutions portées par l'intelligence artificielle pourraient se heurter aux orientations décidées aux plus hauts échelons du Parti, en soulignant par exemple le côté aventureux de certaines initiatives. On peut donc envisager que son emploi au niveau tactique se réduise à certaines tâches et qu'au niveau opératif ou stratégique, celles-ci soient uniquement du ressort de certains officiers fidèles au Parti. Par ailleurs, maintenir la loyauté et l'agressivité des troupes est le problème essentiel posé aux commissaires politiques. Le développement de la robotisation au niveau tactique pourrait le résoudre en partie. Le nombre de soldats diminuerait et la probabilité de faire face à des contestations se réduirait sensiblement.

D'autres paramètres incitent cependant à nuancer cette vision un peu déterministe. Le développement de l'IA dans les armées va par exemple nécessiter le recrutement de jeunes diplômés. Même s'ils devront avoir montré leur fidélité au Parti pour grimper dans la hiérarchie, ils auront

127. Voir S. A. Ambrose, *Band of Brothers: E Company, 506th Regiment, 101st Airborne from Normandy to Hitler's Eagle's Nest,* New York, Simon & Schuster, 2001 ; V. Davis Hanson, *Carnage and Culture: Landmark Battles in the Rise of Western Power,* New York, Doubleday Books, 2001.

128. E. B. Kania, « Battlefield Singularity: Artificial Intelligence, Military Revolution, and China's Future Military Power », *op. cit.*, p. 17.

acquis une certaine autonomie en apprenant à travailler par eux-mêmes et seront plus éduqués, sachant mieux apprécier la nature des situations selon le contexte. En cas de crise ou de difficultés importantes, ces jeunes cadres pourraient être enclins à privilégier une logique opérationnelle sur une logique politique, surtout s'ils partagent les conclusions suggérées par l'intelligence artificielle dont le caractère « scientifique » pourrait être utilisé comme argument face à la hiérarchie.

En outre, les réponses des militaires chinois aux défis de l'intelligence artificielle ne seront probablement pas identiques entre elles. Elles pourraient être guidées par les rivalités bureaucratiques, avec des acteurs qui tenteront de concilier les directives de haut niveau, les instructions de leurs chefs organiques et les contraintes locales. Les expérimentations indiqueront probablement les meilleurs compromis dans chaque cas[129]. Ils pourront se diffuser à l'ensemble de l'APL si leur efficacité est évidente ou simplement démontrée. Enfin, la robotisation possible de l'APL se heurtera sûrement aux convictions de certains officiers généraux qui considèrent que la relation homme-machine de type « centaure » est la forme la plus évoluée des intelligences futures[130]. Ils rejoignent ainsi l'avis de certains de leurs homologues occidentaux.

Est-ce à dire que les doctrines d'emploi de l'intelligence artificielle des différentes armées se rapprocheront dans l'avenir plutôt qu'elles ne s'opposeront, et que les pratiques qui auront fait leurs preuves s'imposeront naturellement à tous ? Les armées européennes adoptèrent toutes le système du corps d'armée après les victoires écrasantes de Napoléon. Elles s'inspirèrent toutes aussi de la Wehrmacht pour combiner avions et chars après les succès de la *Blitzkrieg* en 1940 et 1941, avec bien sûr des arrangements particuliers selon les nations[131]. Les doctrines entre armées de niveau comparable pourraient donc converger plutôt que diverger à terme. C'est une possibilité pour Robert Work, qui va même beaucoup plus loin en déclarant « que si nous forçons [...] un adversaire qui est une puissance autoritaire à adopter les concepts opérationnels et organisationnels de la stratégie de compensation, cela suscitera des changements dans leur appareil militaire et finalement dans leur société qui feront que les probabilités de se combattre seront moins

129. *Ibid*.
130. E. B. Kania, « Battlefield Singularity: Artificial Intelligence, Military Revolution, and China's Future Military Power », *op. cit*., p. 18.
131. Pour les différences entre l'art opérationnel soviétique et allemand : J. Lopez, *Berlin : les offensives géantes de l'armée rouge, Vistule-Oder-Elbe, (12 janvier-9 mai 1945)*, Paris, Economica, 2009.

importantes[132] ». Nul besoin de hackers pour entraver le fonctionnement de l'APL et amoindrir ses performances. C'est l'intelligence artificielle elle-même qui pourra être le virus qui sapera toute l'organisation autoritaire du Parti communiste chinois.

Intelligence artificielle forte et transformation de la guerre

L'introduction de technologies de ruptures au sein des forces armées déclenche régulièrement les mêmes questions. Vont-elles bouleverser les formes de la guerre ? Vont-elles changer la nature de la guerre ? La réponse est souvent positive dans le premier cas, comme le montre la littérature sur les révolutions militaires[133], mais toujours négative dans le second. La définition générale de Clausewitz, qualifiant la guerre « d'acte de violence engagé pour contraindre l'adversaire à se soumettre à notre volonté » n'a jamais été remise en cause par une quelconque technique.

D'éventuels progrès dans la mise au point d'une intelligence artificielle forte pourraient-ils renouveler les réponses à ces questions ? De telles intelligences seraient capables de brasser encore plus d'information, de les relier, d'établir de meilleures connexions entre elles, de tester et d'évaluer les options les plus favorables. À la manière des prévisions météorologiques, elles pourraient énoncer à encore plus long terme la probabilité des événements à venir, avec une précision d'autant plus notable qu'on se rapprocherait de l'échéance.

De l'anticipation à la guerre préventive

Cette meilleure capacité d'anticipation pourrait notamment se traduire par un nouvel intérêt porté aux *Effect-Based Operations* (EBO) dans les options préférentielles des stratèges. Les EBO sont définies comme des opérations conçues et planifiées dans un cadre systémique[134]. Il s'agit d'évaluer la gamme complète des effets directs, indirects ou en cascade qu'on peut atteindre par l'application d'instruments militaires, diplomatiques, psychologiques et économiques et de choisir les meilleurs[135]. Imaginées après la guerre du Golfe de 1991, les EBO avaient

132. C. Pellerin, « Work: Human-Machine Teaming Represents Defense Technology Future », *DoD News*, Defense Media Activity, 8 novembre 2015, disponible sur : www.defense.gov.
133. A. F. Krepinevich, « Cavalry to Computer: The Pattern of Military Revolutions », *The National Interest*, automne 1994, n° 37.
134. P. Coquet, « Opérations basées sur les effets : rationalité et réalité », *Focus stratégique*, n° 1, Ifri, octobre 2007, disponible sur : www.ifri.org.
135. P. K. Davis, *Effects-Based Operations: A Grand Challenge for the Analytical Community*, Santa Monica, RAND Corporation, 2001.

pour but de reprendre et d'améliorer les principes qui avaient guidé la campagne aérienne. Il ne s'agissait plus de détruire une partie du potentiel économique de l'adversaire, de chercher systématiquement l'attrition des forces armées ennemies, mais d'agir sur les différents systèmes qui concourraient au fonctionnement des unités militaires ou à la vie du régime politique adverse pour les paralyser. L'essentiel de la planification revenait à analyser les vulnérabilités de ces systèmes et à déterminer les effets pervers ou secondaires des frappes pour mieux les corriger. Les EBO ont connu leur heure de gloire au début de ce siècle avant d'être violemment critiquées en 2008 par le général Mattis, alors commandant suprême pour la transformation dans l'OTAN, pour avoir inspiré le plan de frappes déficient des Israéliens contre le Hezbollah et troublé la planification interarmées[136]. Mattis estimait que la guerre était d'abord le royaume du chaos et qu'il était impossible d'atteindre le degré de prédictibilité annoncé par les EBO.

Une intelligence artificielle avancée pourrait-elle faire mieux ? C'est possible, même si elle n'arrivera pas à bannir l'incertitude et le chaos[137]. Une IA forte pourrait obtenir sur les organisations complexes le même type de résultats que ceux attendus prochainement sur le fonctionnement des individus. Le modèle que proposa le général McChrystal pour décrire l'insurrection afghane pourrait être mieux appréhendé. Ces capacités d'anticipation pourraient amener à privilégier les guerres préventives, à guider la décision en amont même du militaire[138]. Les algorithmes tiendraient alors un rôle similaire à celui des *précogs* du roman d'anticipation de Philip K. Dick *Minority Report*. Ils joueraient aux oracles en signalant les tensions et les probables risques de conflit à venir avec d'autres entités politiques[139]. Les militaires pourraient être envoyés sur certains théâtres à des fins de prévention ou, à la manière des agents de Précrime dans le roman, dans un but de coercition. Comme l'a précisé Emmanuel Macron, l'homme politique devra toujours assumer la responsabilité de sa décision[140]. Si la machine sait évaluer, ce sera à lui, ou aux chefs militaires dans d'autres cas, de convaincre et de donner du sens aux actions.

136. J. N. Mattis, « USJFCOM Commander's Guidance for Effects-based Operation », *Parameters,* vol. 38, n° 3, automne 2008, p. 18-25. Voir la réponse suivante : M. D. Henriksen, « A Misapplied and Overextended Example: J. N. Mattis's Criticism of Effects-Based Operations », *Air & Space Power Journal*, septembre-octobre 2012, p. 118-131

137. P. Jensen, *Pourquoi la société ne se laisse pas mettre en équations*, Paris, Seuil, 2018.

138. A. C. Enthoven et K. Wayne Smith, *How Much is Enough? Shaping the Defense Program*, *op. cit.*, p. 19.

139. P. K. Dick, *Rapport minoritaire*, Paris, Folio, 2009.

140. « Interview du Président de la République, Emmanuel Macron, pour *Wired* sur l'intelligence artificielle », Présidence de la République, 3 avril 2018, disponible sur : www.elysee.fr.

Les affrontements entre IA

La multiplication de machines d'intelligence artificielle avancée au sein des forces armées pourrait provoquer à terme un affrontement tactique entre deux unités automatisées conduites par des algorithmes. À quoi ressemblerait un tel combat ? Quels principes tactiques pourraient être suivis ?

Une expérience menée au sein du programme *Google Brain* à partir de l'envoi de messages chiffrés par une clé de 16 bits a montré que deux intelligences artificielles pouvaient établir un protocole cryptographique sécurisé entre elles, qui ne pouvait être percé par d'autres intelligences artificielles[141]. Un tel résultat, qui demande à être confirmé à une plus large échelle, est prometteur et peut stimuler la mise en réseau d'intelligences artificielles au sein de systèmes complexes. Pour autant, le manque d'expérience dans le domaine de la coopération ou de la lutte entre IA laisse une fois encore le champ des réponses très ouvert. L'exemple des deux bots informatiques qui interagirent lors de la mise aux enchères d'un livre de biologie sur la plateforme Amazon en 2011 est souvent évoqué pour dénoncer les risques d'escalade incontrôlée lors de tels affrontements. Chaque bot répliqua de manière instantanée aux avances de l'autre, de sorte que ce livre fut proposé au prix record de 23 698 655,93 dollars[142].

Le monde de la finance, qui emploie depuis longtemps des systèmes automatisés pour diminuer les temps de latence et optimiser ses gains offre d'intéressantes clés de lecture pour ces affrontements. Une des craintes les plus fréquentes est celle de l'entrée en résonance d'IA utilisant des bases de données et des algorithmes. Face à un choc, elles tireraient immédiatement les mêmes conclusions et pourraient amplifier très rapidement et très dangereusement des mouvements de retrait ou de ventes à perte, préparant le terrain pour une crise plus importante[143]. Ce risque serait peut-être moins sensible dans le domaine militaire, où les algorithmes génériques pourraient avoir été conçus ou au moins avoir été modifiés par des experts locaux pour des raisons de sécurité nationale. Ce type de chaos ne serait pas une fatalité. Un duel entre intelligences artificielles pourrait alors davantage refléter les capacités d'accès à l'information des deux entités militaires, l'expertise des programmeurs ou les biais introduits par les responsables militaires dans les

141. T. Berthier, « Les apports de l'intelligence artificielle en cybersécurité et cyberdéfense », *op. cit.*, p. 40.
142. P. Scharre et M. C. Horowitz, « Artificial Intelligence: What Every Policymaker Needs to Know », *op. cit.*, p. 14
143. « Artificial Intelligence and Machine Learning in Financial Services: Market Developments and Financial Stability Implications », *Financial Stability Board*, 1er novembre 2017, disponible sur : www.fsb.org.

algorithmes afin qu'ils respectent les procédures habituelles et les cultures propres du combat.

Par ailleurs, dans l'environnement de la finance, le volume et la vitesse de transmissions des ordres reflètent les capacités des systèmes automatisés. En un clignement d'œil, soit 350 millisecondes, 7 000 ordres sont placés à travers le monde. Cinq microsecondes suffisent pour l'exécution d'une transaction[144]. Réduire ces minuscules intervalles de temps peut permettre de maximiser ses gains, car le fait d'agir avant ses concurrents offre la possibilité de saisir en premier les opportunités. Être équipé de câblages en fibre optique, disposer ses ordinateurs très près des serveurs raccourcit les délais d'échange et de propagation des signaux. Un tel souci d'optimisation du temps de transmission pourrait également être partagé par le monde militaire. Si la distance qui sépare les drones et les opérateurs n'a pour l'instant pas entravé les opérations, elle pourrait devenir plus sensible si des systèmes automatisés s'affrontaient en étant commandés par des intelligences artificielles éloignées. Celle qui « dégainerait » le plus vite aurait alors un avantage décisif sur l'autre, notamment si des armes à énergie dirigée ou hypersoniques étaient employées. Projeter des forces à distance pourrait poser alors des problèmes face à un défenseur bien équipé. Cette vulnérabilité pourrait pousser dans certains cas au déploiement d'intelligences artificielles décentralisées sur les effecteurs et limiter la coordination d'une manœuvre générale.

Vers un changement de nature de la guerre ?

Comme l'indique Frank G. Hoffman, ancien Marine et chercheur à la *National Defense University*, « tant que les humains seront responsables de la direction de la guerre, de l'écriture des codes et du fonctionnement et de l'entretien des machines, la guerre restera un instrument de la politique et dans les mains des combattants. [...] Les éléments les plus significatifs de la guerre – violence, facteurs humains et hasard – demeureront certainement.[145] » Analysant l'impact de la diffusion des intelligences artificielles faibles dans les armées, il reconnaît que la plupart des domaines de la guerre seront touchés par la diffusion de cette technologie, mais assure que les fondements de la guerre seront préservés.

144. L'auteur remercie Bertrand Quiminal pour avoir attiré son attention sur ce point. Lire : D. Larousserie, « La finance à la vitesse de la lumière », *Le Monde*, 27 mai 2015.
145. F. G. Hoffman, « Exploring War's Character and Nature: Will War's Nature Change in the Seventh Military Revolution? », *Parameters*, vol. 47, n° 4, hiver 2017-2018, p. 31.

On le suivra volontiers pour le court et moyen terme, bien qu'avec une nuance : la conclusion des raisonnements de l'intelligence artificielle peut différer profondément de ceux des êtres humains. Sa « pensée » est parfois peu compréhensible par l'homme, non seulement du fait des techniques de codage déjà évoquées, mais aussi parce que l'approche par l'IA d'un problème donné est différente de celle d'un humain. Les parties d'échecs ou de go jouées par des machines offrent ainsi des exemples surprenants. Le logiciel *Alphazero* sacrifia délibérément un fou lors d'une partie d'échecs contre un autre logiciel appelé *Stockfish*, qui tenait une position défensive particulièrement forte. Ce mouvement étonna des joueurs très confirmés qui ne saisissaient pas l'intérêt de perdre une telle pièce sans contrepartie. Ils réalisèrent après que le logiciel avait pris le contrôle d'une zone dont il tira profit pour lancer une attaque. *Alphazero* parvient à fragiliser le dispositif de *Stockfish* et infligea finalement un mat au roi adverse[146]. De même, alors qu'il était opposé pour son deuxième match au logiciel *AlphaGo*, Lee Sedol, considéré comme le meilleur joueur mondial de go, quitta la table de la partie pendant quinze minutes, tant il fut déstabilisé par un mouvement de la machine. Un tel coup lui était incompréhensible. Il n'avait une probabilité que de 1 sur 10 000 d'être joué par un être humain. La machine était-elle en panne ? Fallait-il l'annuler ? Ce coup très original permit pourtant à *AlphaGo* de triompher lors de cette partie[147]. À chaque fois, la machine agit pour gagner, pour répondre à la finalité de sa programmation. Le nombre de voies explorées par les logiciels est bien plus important que celles qu'un être humain peut parcourir. Les possibilités d'interactions pressenties entre des paramètres étrangers ou des événements éloignés par les programmes informatiques dépassent largement les capacités humaines. Toute une gamme d'autres possibles s'ouvre soudainement qui dérouteront nécessairement les opérateurs et les responsables.

Par ailleurs, la stratégie proposée par l'intelligence artificielle ne sera pas influencée par les sentiments que les hommes peuvent connaître quand ils élaborent leurs plans. Leurs expériences de vie, leur tolérance aux risques, leur colère ou leurs craintes influencent leurs choix de manière consciente ou inconsciente. La fatigue, l'épuisement, le stress perturbent leurs décisions. Ils sont contraints par différents groupes d'intérêt qui encouragent la conformité. Les stratégies élaborées par les hommes sont une résultante des interactions entre leur esprit et leur corps[148]. Une intelligence artificielle avancée sera étrangère à tous ces facteurs et ne sera

146. M. Rawson, « Techmate: How AI Rewrote the Rule of Chess », *Financial Times*, 4 février 2018.
147. C. Metz, « In Two Moves, *AlphaGo* and Lee Sedol Redefined the Future », *Wired*, 16 mars 2016, disponible sur : www.wired.com.
148. K. Payne, *Strategy, Evolution, and War: From Apes to Artificial Intelligence, op. cit.*

que logique. Elle sera « un pur esprit », fonctionnant à partir des règles qu'elle aura elle-même élaborées. La question est alors de savoir si le conflit et sa résolution peuvent être toujours envisagés d'une manière classique ou, si en chassant les faiblesses humaines du champ de bataille, la guerre en est transformée.

D'un point de vue théorique, Clausewitz définit la guerre comme le résultat de l'interaction entre les trois éléments d'une trinité composée par le peuple et ses passions, le politique et son entendement, et enfin le général et son armée, qui incarnent la libre activité de l'esprit, le courage et le talent dans les jeux des probabilités et du hasard. À mesure que l'intelligence artificielle deviendra forte, elle réduira justement ce libre jeu de l'esprit en désignant les meilleures pratiques. Tel un GPS actualisant la circulation pour un conducteur de voiture, l'intelligence artificielle indiquera le chemin le mieux adapté à suivre, et pourra proposer le trajet le plus rapide ou le moins onéreux en carburant. Ne pas suivre ses indications aura un coût. Elle bornera les effets du hasard, en les prévenant ou en s'adaptant à leurs conséquences. Elle limitera les expressions du courage en favorisant l'automatisation. Les qualités et les vertus qui définissent un général et son armée dans l'acception clausewitzienne s'estomperont progressivement. Les fonctions qu'ils tiennent seront en partie assurées par des machines sachant se saisir des problèmes et gérer l'environnement. Le maniement de l'entendement ne sera plus le simple monopole du politique. Il s'étendra à la sphère militaire par l'intermédiaire des machines qui agiront comme les principaux stratèges.

Il se pourrait alors que les connexions entre le politique et le militaire se simplifient. Les deux entités emploieraient une méthode commune pour arriver à un but partagé. Le recours à la violence serait ajusté au niveau suffisant pour satisfaire les besoins politiques. La guerre pourrait alors ne plus avoir de grammaire propre, de dynamique spécifique. La politique imposerait sa présence à tous les niveaux de la guerre, jusqu'au plus petit détail sub-tactique. Le guerrier deviendrait alors une figure du passé, remplacée par des opérateurs s'assurant que la marche des événements est conforme à celle exprimée par le politique, et parfaitement traduite par la machine. La guerre existerait toujours, mais le guerrier aurait disparu.

Conclusion

À la fin de ce bref voyage au cœur de l'intelligence artificielle et de ses conséquences futures sur l'art de la guerre, un rappel sur le caractère hypothétique des évolutions présentées paraît à nouveau indispensable. Par certains aspects, l'intelligence artificielle représente bien plus qu'elle-même. Parce que son développement est encore incertain, parce que sa marche peut emprunter des voies très différentes, chacun peut placer en elle ce qu'il souhaite, comme ses peurs, ses désirs, ses espoirs, ses croyances ou ses valeurs.

Néanmoins, un des grands apports de l'intelligence artificielle sera, à notre sens, de remettre en cause nombre de certitudes et de contraindre les militaires à débattre sur le fond de notions qui restaient jusqu'alors ignorées ou trop abstraites, jusqu'alors laissées aux savants ou aux philosophes. Qu'est-ce que l'intelligence ? Faut-il vraiment être intelligent pour gagner une bataille ? La persévérance, le don de soi et le courage sont-ils parfois plus importants ? Sommes-nous libres ou déterminés ? Est-il réellement possible d'anticiper nos intentions et la manière dont nous agissons sur le champ de bataille ? Certains individus sont-ils plus imprévisibles et créatifs que d'autres ? Doivent-ils être valorisés dans les institutions militaires, même si leur sens de la hiérarchie n'est pas irréprochable ?

Autant de questions pour lesquels des éléments de réponse existent déjà, mais qui vont être posées avec plus d'acuité à l'avenir. La forme de la coopération homme-machine sera sans aucun doute déterminante pour le verdict. À court et moyen termes, l'homme continuera d'y tenir le rôle décisif, quitte à ce que la machine se voie déléguer de plus en plus de tâches. Mais que se passerait-il si l'homme évoluait à son tour ? Si ses moyens augmentaient ? À écouter certains observateurs, un tel scénario n'a rien à voir avec la science-fiction[149]. Un tel résultat serait obtenu par des manipulations génétiques. Le courant transhumaniste soutient naturellement de telles expériences. Il renverse notre vision de l'être humain et se heurte violemment à l'humanisme traditionnel. Selon ce courant, la nature de l'homme n'est pas achevée[150]. La technique est au service de la liberté et doit permettre de réparer ou d'améliorer l'homme. L'un des buts est de parvenir un

149. V. Tremollet de Villers et L. Alexandre, « *Bienvenue à Gattaca* deviendra la norme », *Le Figaro*, 2 juin 2017. Dans le même temps, seules 13 % des personnes interrogées en Europe feraient le même choix.
150. Le philosophe belge Gilbert Hottois propose aujourd'hui une des visions les plus abouties en Europe de ce mouvement : G. Hottois, *Philosophies et idéologies trans/posthumanistes*, Paris, Vrin, 2017.

jour à « l'amortalité[151] ». L'opposition entre naturel et artificiel serait alors vouée à disparaître.

Si l'homme et la technologie se marient pour évoluer ensemble, la réflexion sur la nature de la relation homme-machine se transformera à son tour. Le combattant sera un cyborg, c'est-à-dire un être humain doté de greffons techniques ou électroniques. La technologie ne sera plus au service de l'homme, mais intégrée à l'homme. Quant à la possibilité de devenir « amortel », elle bouleversera radicalement la manière d'envisager la guerre et donc la mort sur le champ de bataille. Cette perspective deviendra insoutenable, car balayant un des fondements de la nouvelle société. L'intelligence artificielle livrera alors complètement son potentiel, pour le meilleur et pour le pire, succédant à des hommes considérant leur vie comme beaucoup trop précieuse pour être risquée. Lire les romans de science-fiction est peut-être dans ce cas le moyen le plus sûr d'identifier ce que sera l'art de la guerre dans le futur.

151. Allongement radical de la durée de la vie en bonne santé.

ifri
institut français
des relations
internationales