NOTE

Note n° 15/FRS/Consortium OBSAT 35
du 9 janvier 2019

Marché ° 431532/SGA/SPAC/SDA/BPI du 27/02/2017
notifié le 9 octobre 2017
Tranche 2 – réunion de lancement : 3 octobre 2018

Observatoire de l'armée de Terre 2035

Tranche 2 – Note n° 2

Impacts de l'intelligence artificielle dans le champ de bataille sur les fonctions de supériorité opérationnelles de l'armée de Terre à l'horizon 2035

NICOLAS MAZZUCHI – BRUNO LASSALLE – JONATHAN JAY MOURTONT

WWW.FRSTRATEGIE.ORG | 4 BIS RUE DES PATURES 75016 PARIS | TEL : 01.43.13.77.77 | MAIL : CONTACT@FRSTRATEGIE.FR
SIRET 39409553300052 TVA FR74 394 095 533 CODE APE 7220Z FONDATION RECONNUE D'UTILITÉ PUBLIQUE DÉCRET DU 26 FÉVRIER 1993

WWW.EUROCRISE.COM | 8 RUE DE BELLEFOND 75009 PARIS | TEL : 01.49.49.01.23 | MAIL : EUROCRISE@EUROCRISE.COM
SIRET 438 431 207 00036 TVA FR 1743 8431 2070 0036 COPE APE 7022Z

Fiche de synthèse

Les technologies liées à l'intelligence artificielle et celles, connexes, de la robotique automatisée, visent à comprendre – pour la répliquer – la cognition humaine. Dans un contexte militaire, l'introduction de ces technologies aurait très probablement des conséquences majeures, lesquelles sont appréhendables au travers du cadre des FSO de l'armée de Terre. Si l'ensemble des facteurs de supériorité opérationnelle seraient touchés par l'IA et les technologies associées, certains apparaissent plus favorables à une coopération Homme-Machine via l'IA. La compréhension, la coopération, la masse (au travers de la robotique automatisée), l'endurance (en particulier au niveau du MCO prédictif) et l'influence (pour l'élaboration des messages et l'identification des relais) seraient ainsi les FSO les plus susceptibles de bénéficier des apports des technologies liées à l'IA.

Au travers de la grille d'analyse des FSO, il est également possible d'évaluer le potentiel d'utilisation – moyennant des adaptations sur un certain nombre de points – de technologies duales. En effet, les technologies liées à l'IA et à la robotique sont, en l'état de l'art et des recherches, surtout en France et en Europe, avant tout tirées par le secteur civil.

Malgré ces opportunités, il est également nécessaire d'appréhender les vulnérabilités créées par l'utilisation d'IA chez des adversaires potentiels d'une part et par l'introduction des technologies liées à l'IA au sein de l'armée de Terre d'autre part. L'une des principales vulnérabilités ouvertes, en plus de celles liées aux enjeux industriels, technologiques, éthiques ou juridiques, concerne la disponibilité des données nécessaires aux entraînements des IA. Sans un volume et une qualité de données maîtrisées en interne, la qualité des systèmes automatisés serait ainsi fortement limitée.

En ce qui concerne le cadre DORESE des différentes fonctions de l'armée de Terre, l'introduction des technologies liées à l'intelligence artificielle aurait des impacts différenciés dans chacune des fonctions envisagées. Toutefois trois d'entre elles semblent devoir subir plus d'évolutions que les autres. En premier lieu la doctrine doit évoluer afin de prendre en compte les différents degrés d'autonomie des machines et équipements et les conditions dans lesquelles ces degrés d'autonomie peuvent être autorisés. Ensuite l'organisation doit prendre en compte la nécessité de disposer de spécialistes techniques à tous les niveaux – selon les besoins opérationnels et en termes de soutien – disposant des compétences à même de permettre à l'armée de Terre de conserver la

haute main sur ces technologies. Enfin le domaine RH s'avère l'un de ceux où les évolutions devraient être les plus profondes, nécessitant la mise en place de cursus particuliers, en mécatronique notamment, pour les militaires officiers et sous-officiers, ainsi que de processus RH nouveaux pour attirer et fidéliser des spécialistes civils hautement qualifiés.

Un dernier point, pour la clarté du spectre des développements possibles, l'équipe de recherche présente des scénarios prospectifs en annexe. Le lecteur intéressé pourra s'y reporter.

SOMMAIRE

FICHE DE SYNTHÈSE 3

INTRODUCTION 7

1 – DÉFINITIONS 7

1.1 – IA limitée contre IA générale 7

1.2 – La place de l'humain 8

1.3 – L'entraînement des IA, enjeu central 9

2 – L'IA VIS-À-VIS DES FACTEURS DE SUPÉRIORITÉ OPÉRATIONNELLE 11

2.1 – Compréhension 11

2.2 – Coopération 12

2.3 – Agilité 13

2.4 – Masse 13

2.5 – Endurance 14

2.5.1 – Action sur le système logistique/MCO par une vision prédictive 15

2.5.2 – Robotisation d'un certain nombre de fonctions 15

2.6 – Force morale 16

2.7 – Influence 16

2.8 – Performance du commandement 17

3 – VULNÉRABILITÉS À 2035 DE L'ARMÉE DE TERRE FACE À L'IA 18

3.1 – Combattre un adversaire partiellement ou totalement doté d'IA/robots 18

3.2 – Vulnérabilités intrinsèques du développement de l'IA dans l'armée de Terre 19

3.2.1 – Facteurs industriels 19

3.2.2 – Facteurs logistiques et communication 20

3.2.3 – RH et data 21

A.– Leurrage d'IA par injection de fausses informations 22

B.– Disponibilité des données trop faible 22

3.2.4 – Facteurs éthiques et légaux 23

4 – IMPACTS SUR LE MODE DE FONCTIONNEMENT DE L'ARMÉE DE TERRE 24
4.1 – Doctrine 24
4.2 – Organisation 25
4.2.1 – Quel positionnement pour l'IA dans l'armée de Terre ? 25
4.2.2 – Différencier les capacités IA et robotique selon les échelons de commandement 26
4.3 – RH 27
4.4 – Entraînement 29
4.5 – Soutien 30
4.5.1 – Processus de contrôle des performances des algorithmes 30
4.5.2 – Processus de mise à jour des algorithmes 30
4.6 – Equipements 30

CONCLUSION 31

ANNEXE – SCÉNARIOS PROSPECTIFS 33

SCÉNARIO A – DÉVELOPPEMENT LIMITÉ DE L'IA TIRÉ PAR LE CIVIL 33
A.– Descriptif 33
B.– Tendances 35

SCÉNARIO B – ACCUEIL ASSUMÉ DU NOUVEAU PARADIGME 36
A.– Descriptif 36
B.– Tendances 38

SCÉNARIO C – ADAPTATION DE L'ARMÉE DE TERRE DANS UN CONTEXTE DE PEUR DE L'IA ET DE LA ROBOTIQUE MILITAIRE 40
A.– Descriptif 40
B.– Tendances 41

INTRODUCTION

L'intelligence artificielle (IA) qui a pour ambition la compréhension de la cognition humaine afin de créer des processus comparables, regroupe une famille de technologies aux multiples ramifications. Même si l'intelligence artificielle peut avant tout être vue comme une machine qui apprend pour automatiser des tâches, le foisonnement technologique couvert par ce terme d'IA recoupe de nombreuses sous-branches qui peuvent se révéler potentiellement utiles à l'armée de Terre. Afin d'évaluer l'impact potentiel de l'IA – et des domaines connexes – sur l'armée de Terre à l'horizon 2035, il convient de regarder comment ces IA peuvent contribuer aux facteurs de supériorité de l'armée de Terre et, en miroir, quelles seraient les problématiques ouvertes par une certaine généralisation de leur emploi au sein des forces afin de préparer le combat numérisé puis infovalorisé qui se profile.

I – Définitions

I.1 – IA limitée contre IA générale

Le premier élément qu'il convient de définir concerne le niveau d'intelligence artificielle. Deux grands niveaux sont envisageables, d'une part les IA limitées qui sont optimisées pour la réalisation automatisée d'une seule tâche – lesquelles existent déjà – et les IA générales, multitâches et multi-capteurs capables d'une grande autonomie de décision et d'action – qui n'existent qu'au stade prospectif. Les deux types de machines apprenantes sont en réalité assez éloignés l'un de l'autre.

Les IA limitées qui comprennent les systèmes experts – médicaux et autres – apparus dans le monde professionnel dans les années 1980, sont bien connues et ne sont au fond que des systèmes de traitement optimisés de données. Aidant les professionnels humains à accomplir des tâches fondées sur la reconnaissance de certains éléments, ce sont des systèmes dont le socle est un procédé de traitement de type *big data*. Pour le moment les IA limitées sont en outre spécialisées dans la variété des sources de données qu'elles peuvent utiliser. Les meilleurs exemples de ces IA sont les systèmes de jeu de type *Deep Blue* ou *Alpha Go*, automates dont le niveau d'expertise sur un point précis dépasse celui des humains dans des environnements aux règles rigides. Très efficaces comme soutien

dans le pré-tri ou la préanalyse, les IA limitées ne peuvent remplacer les humains dans les tâches complexes. En ce sens elles agissent comme des « cyber-prothèses »[1].

Les IA générales seraient des systèmes fondés avant tout sur la fusion d'expériences multi-capteurs. Reposant sur la combinaison de données de natures diverses, les IA générales – souvent envisagées dans le contexte d'une robotique plus ou moins autonome[2] – seraient capables de dépasser les capacités humaines, y compris dans l'aspect adaptatif des humains. La robotique aiderait en ce sens à disposer de capteurs multiples embarqués, apportant à un même système des données de natures très diverses (images, sons, vidéos, systèmes fondés sur le toucher, etc.). Les IA générales soulèvent les critiques de nombreux chercheurs et personnalités, tel Elon Musk, sur leur côté potentiellement dangereux pour l'être humain. En dépassant les capacités humaines avec une liberté d'action importante, les IA générales pourraient, selon leurs détracteurs, signifier à terme le remplacement de l'humanité comme espèce dominante de la planète. De fait les travaux sur l'IA sont, de manière générale, suspectés de vouloir entraîner l'Homme vers la création d'IA générales[3]. Les études conduites depuis quelques années estiment la probabilité d'une telle IA d'ici à environ 80-120 ans[4].

1.2 – La place de l'humain

Dans ce contexte trois grands types de relations peuvent être envisagés entre humain et machine selon le degré d'autonomie accordé à cette dernière dans la décision. Le premier, suivant la terminologie anglo-saxonne des « niveaux d'autonomie »[5], est dit *human-in-the-loop*. L'être humain est ici pleinement aux commandes du système et aucune action d'importance ne peut être entreprise sans une action effective de celui-ci. Le système automatisé est responsable de l'identification des différents éléments du champ de bataille, de leur suivi et propose des solutions à l'humain qui est seul en contrôle. Les systèmes antimissiles Aegis de Lockheed-Martin, en service dans l'US Navy, fonctionnent suivant ce principe[6].

---

[1] C'est notamment le cas sur le Merkava 4 Barak de Tashal pour lequel le système d'IA est conçu pour décharger l'équipage d'un certain nombre de tâches, en particulier en combat urbain, sans toutefois envisager un blindé qui fonctionne de manière autonome : https://nationalinterest.org/blog/buzz/meet-israels-new-ai-enhanced-tank-barak-26906

[2] *De facto* la robotique collaborative (ou cobotique) serait également fondée sur une certaine adaptabilité du cobot venant en soutien de l'humain, notamment par une capacité d'anticipation des tâches que celui-ci doit accomplir. Il n'est ainsi pas étonnant que le premier domaine de développement de la cobotique soit les usines 4.0, environnements très balisés et prévisibles.

[3] Sans compter les critiques sur les éléments connexes promus par certaines entreprises comme Google sur des projets de type transhumaniste dans lesquels l'IA jouerait un rôle majeur.

[4] https://arxiv.org/pdf/1705.08807.pdf

[5] Suivant le DoD *Unmanned Systems Integrated Roadmap* 2017-2042 de 2017.

[6] Il s'agit ici du fonctionnement courant, le système Aegis ayant la possibilité d'être employé en autonomie complète (*human-out-of-the-loop*), même si ce mode n'est jamais employé en opérations.

Le second niveau est dit *human-on-the-loop*. Il s'agit ici pour l'humain d'effectuer une supervision des actions du système. La validation de l'Homme est toujours requise pour l'engagement des fonctions létales par exemple, mais le processus est davantage automatisé en termes de fonctionnement routinier et de désignation précise des cibles. Le système peut d'ailleurs fonctionner dans ce cas en double contrôle avec un opérateur humain, comme c'est le cas des drones antiradars suicides israéliens IAI Harop qui peuvent à la fois être guidés par un pilote-désignateur ou agir de manière automatique en se calant sur les émissions radar dans une zone donnée[7].

Le niveau le plus automatisé est dit *human-out-of-the-loop*. Il correspond à un système autonome qui prend lui-même ses propres décisions une fois activé par l'agent humain. Dans ce type de système militaire, s'il était utilisé dans la fonction combat, la machine traiterait elle-même toutes les phases de l'action, y compris la décision d'ouverture du feu. Un tel système n'est pas en fonction dans le monde militaire puisqu'il reviendrait à laisser une machine décider de la vie et de la mort[8]. Toutefois ces systèmes ne sont pas totalement écartés des recherches dans le sens où ils permettraient, par une véritable faculté de décision, d'opérer dans des environnements non-permissifs en termes de communications.

Ces trois degrés d'autonomie sont une manière efficiente de classifier les intelligences artificielles dans le contexte militaire, par le niveau de décision qui est laissé à l'opérateur humain. Celui-ci est, dans les deux premiers cas, pleinement responsable du respect des règles d'engagement en opération, alors que dans le dernier cas il n'est responsable – au sens opérationnel et pas juridique – de la programmation de ces dernières[9].

1.3 – L'entraînement des IA, enjeu central

Une autre problématique d'importance se profile vis-à-vis des intelligences artificielles : leur nécessité de disposer de jeux de données les plus exhaustifs et importants possibles pour l'entraînement. Une IA est avant tout une machine qui apprend au travers de corrélation de données. Ces mêmes données acquièrent donc en ce sens une valeur cruciale pour la performance des IA ainsi que leur fiabilité[10]. Dans le domaine militaire, cette problématique est d'autant plus cruciale que les données en question se rapportent à

[7] IAI s'est fait une spécialité de ce type d'engins (*loitering ammunitions*) qui fonctionnent de manière automatisée avec le Harpy, le Green Dragon ou le Rotem.

[8] Ce qui poserait de nombreux problèmes juridiques en termes de responsabilité pour attribuer la décision (fabricant de la machine, organisme l'opérant, etc.).

[9] Sur la question de la place de l'humain et ses enjeux, voir P. Scharre, *Army of None: Autonomous Weapons and the Future of War,* New York, Norton, 2018.

[10] La vague technologique actuelle de l'IA et la sortie de « l'hiver de l'IA » s'expliquent par deux phénomènes concomitants : l'augmentation de la capacité de calcul des processeurs et la disponibilité de gigantesques volumes de données structurées.

des opérations, à des personnels ou à des doctrines ; la plupart de ces éléments faisant l'objet d'une classification plus ou moins forte.

Au-delà même de la nature des données servant à leur entraînement, se pose la question de la manière dont celui-ci est effectué. Deux grandes familles existent en effet : les entraînements supervisés et non-supervisés[11]. Dans le premier cas, il s'agit de contrôler l'apprentissage de l'IA par un acteur extérieur qui analyse les résultats des reconnaissances de données par un système de récompenses/punitions. La structuration du mode de réflexion de la machine est ainsi opérée par le contrôleur qui s'assure de l'adéquation de celui-ci par rapport aux exigences du système. Dans le second cas, la machine opère seule face aux jeux de données et doit en tirer des corrélations pertinentes.

L'entraînement supervisé est ainsi consommateur en termes de personnel spécialisé puisqu'il nécessite des spécialistes de l'IA pour mettre en œuvre et contrôler l'accès des machines aux données, ainsi que les résultats obtenus. En outre, dans les deux types d'entraînement mais plus spécifiquement dans le cas des entraînements supervisés, le problème de l'oubli catastrophique n'est toujours pas complètement résolu[12]. L'oubli catastrophique qui consiste, pour une IA, à devoir recommencer son apprentissage à chaque nouvelle tâche, est une limite importante à la polyvalence des systèmes, pourtant nécessaire dans un usage militaire.

L'entraînement non-supervisé offre des possibilités intéressantes en termes d'agilité. En effet en permettant à l'IA de découvrir selon ses propres modalités, les corrélations existantes entre des données de natures parfois différentes, il lui donne la possibilité de s'adapter à des environnements moins balisés. Les forces armées étant amenées à intervenir sur des théâtres divers, souvent hors des zones où la signalisation est forte[13], l'entraînement de type non-supervisé semble plus adapté aux IA qui doivent être déployées au plus près des forces. Toutefois l'entraînement non-supervisé pose une série de problèmes qui, dans le cas de l'armée de Terre, peuvent devenir critiques. Le plus important d'entre eux est l'incapacité, pour les ingénieurs-programmeurs spécialistes de l'entraînement, d'appréhender les langages spécifiques créés par les IA pour leur propre compréhension. En ce sens, il est impossible d'évaluer finement le degré de fiabilité d'un système de reconnaissance d'objets/éléments, ce qui dans le monde militaire s'avère difficilement

[11] Auxquels se rajoutent des formes particulières comme l'apprentissage par renforcement.

[12] Deepmind, filiale spécialisée de Google en IA, a néanmoins annoncé avoir fait une percée importante en ce domaine en 2017, grâce à un type particulier d'apprentissage des réseaux de neurones.

[13] Que ce soit dans des environnements où il n'existe pas ou peu d'infrastructures ou à cause de la destruction de celles-ci.

compatible avec des nécessités opérationnelles. Le conflit qui est par essence un domaine non-balisé, doit ainsi articuler les problématiques de la plasticité (entraînement non-supervisé) contre la fiabilité (entraînement supervisé)[14].

Ces problématiques doivent également prendre en compte des intrants technologiques supplémentaires issus de technologies connexes, concernant le stockage et le traitement des données. Le « renouveau » actuel de l'IA n'a ainsi été possible, après plusieurs « hivers », que grâce à la combinaison de grandes capacités de calcul informatique à un prix abordable – suivant la loi de Moore –, et à une disponibilité des données extrêmement grande due à l'explosion de la communication numérique. D'ici quelques années, les technologies liées à l'informatique quantique pourraient, en modifiant radicalement l'accès aux capacités de calcul, permettre aux technologies de l'IA de prendre une nouvelle dimension. De même, la potentielle convergence NBIC[15] ouvre des possibilités étendues en termes d'accès aux données ainsi qu'à leur utilisation.

2 – L'IA vis-à-vis des facteurs de supériorité opérationnelle[16]

2.1 – Compréhension

La première application de l'IA dans les systèmes militaire futurs serait probablement dédiée au renseignement (et plus largement aux systèmes ISR). En effet l'IA permettrait d'effectuer un prétraitement des données recueillies par les différents capteurs (techniques et humains) avant intervention de l'analyste ou de l'interprète spécialisé. En termes RH, l'IA faciliterait ainsi la diminution du volume de formations spécifiques longues, comme celle des interprètes photographiques. Sans remplacer ces derniers, des systèmes de traitement automatisé de reconnaissances de formes, disposant des bases de données idoines[17], seraient de parfaits auxiliaires des interprètes images. Différents projets de ce type existent déjà comme le système MAVEN employé pour le ciblage des agents et infrastructures de Daech par les drones américains[18]. En outre, la gestion des

[14] Un bon exemple de dérapage d'IA non supervisée a pu être observé avec le robot conversationnel Tay, de Microsoft en 2016. En à peine 8 heures d'existence, celui-ci avait largement dérivé vers une vision raciste et extrémiste du monde, obligeant Microsoft à arrêter l'expérience. Cet exemple illustre également la problématique de la qualité des données pour l'entraînement, Tay ayant évolué suite aux conversations qu'il avait eues avec des internautes sur Twitter.

[15] Nanotechnologies, biotechnologies, informatique et sciences cognitives.

[16] Pour une autre lecture des apports de l'IA dans le domaine militaire : J-C. Noël, *Intelligence artificielle, vers une nouvelle révolution militaire ?* Paris, IFRI, 2018.

[17] L'apprentissage par renforcement supervisé est ici particulièrement utile pour l'identification des matériels militaires, ou des différents objets dont la forme est connue (infrastructures, réseaux électriques ou de communication, etc.).

[18] https://www.c4isrnet.com/it-networks/2018/07/27/targeting-the-future-of-the-dods-controversial-project-maven-initiative/

données massives par agents complexes donne lieu d'envisager une fusion des données de natures différentes (par exemple ROIM et ROEM) dans des produits particuliers de type GEOINT, immédiatement disponibles pour les forces. Si l'IA ne permettait pas de s'abstraire de l'analyse humaine dans les produits de renseignement les plus analytiques, elle permettrait néanmoins l'accélération de la disponibilité de l'information pour ces mêmes analystes.

En ce sens, l'armée de Terre ne se singularise pas des autres forces armées, car elle utilise pour ses opérations des capteurs de toutes natures multi-milieux. En outre, la mutualisation des données au niveau de la DRM ne laisse pas entrevoir une réelle spécificité Terre, même si le système Scorpion est fondé sur la compréhension et l'infovalorisation.

2.2 – Coopération

La coopération – en tant que faculté d'agir et de combattre avec l'ensemble des acteurs de la crise ou du conflit – nécessite de disposer de systèmes de communication particulièrement robustes, pour lesquels la cybersécurité est une préoccupation majeure, afin de disposer d'une permanence des communications pour délivrer les messages avec le bon niveau de confidentialité et dans le bon timing. La cybersécurité des systèmes d'information peut bénéficier de grandes avancées, grâce aux technologies liées à l'intelligence artificielle. Plusieurs grands usages peuvent ainsi être inférés, qu'il s'agisse d'intervenir sur le réseau lui-même pour détecter les transferts de données dans certaines zones (*advanced DPI*), sur les utilisateurs du réseau pour détecter les comportements anormaux (*User Behavior Analysis*), ou en tant que défense active pour détecter les anormalités (attaques par architectures de données fictives, pouvant donner lieu à de *l'AI spoofing* également)[19]. C'est l'un des axes principaux de travail de la DARPA, en particulier au travers du *Cyber Grand Challenge* de 2016, qui visait à écrire un algorithme qui soit en même temps capable d'opérer une défense de son propre système et une attaque du système adverse.

Au-delà des questions de sécurité proprement dites, l'IA favoriserait également la mise en œuvre des réseaux agiles de télécommunication capables de se reconfigurer tout en disposant d'un niveau de sécurité important. Le projet MANET de la DARPA, dont la dernière version publique date de 2013[20], cherche, au travers d'un système intelligent distribué, à mettre en œuvre un protocole différent du protocole IP actuel qui autoriserait un partage de données important sur le champ de bataille, en évitant une éventuelle

[19] Voir infra et http://binaire.blog.lemonde.fr/2018/09/07/detecter-le-faux-securiser-le-vrai/

[20] https://www.darpa.mil/news-events/2013-04-30

altération localisée et temporaire de l'Internet[21]. La crainte d'une supériorité de la part des autres grandes puissances militaires (Chine et surtout Russie) dans le domaine de la guerre électronique, pousse les États-Unis à investir massivement ce champ de recherche, comme le démontre la *Third Offset Strategy*. Il y a donc ici un espace majeur de travail sur les questions d'intelligence artificielle mais qui, par essence, n'est que peu spécifique au domaine terre.

2.3 – Agilité

L'agilité – en tant que capacité à répondre à l'évolutivité de l'environnement – s'envisage principalement aux échelons de commandement de mission, de théâtre ou d'opération (CPCO). L'IA dans ce contexte est envisagée en tant que système permettant un raccourcissement de la boucle OODA, en conjonction avec les FSO « compréhension » et « performance du commandement ». L'utilisation de systèmes d'aide à la décision à certains échelons, pour la simulation des comportements ennemis (au niveau J5), ou le conseil au décideur par exploration des hypothèses possibles (au niveau J35)[22], se révèle très utile.

L'IA donnerait également la possibilité de modéliser les comportements sociaux généraux et individuels, nécessaires à l'approche globale des opérations, même s'il reste important de ne pas « mathématiser » à outrance la conduite de celle-ci, au risque de reproduire l'erreur des États-Unis, lors de la seconde phase de la guerre du Vietnam[23].

S'adapter à l'environnement c'est aussi savoir utiliser des modes dégradés ou des systèmes disposant d'un important degré d'autonomie, en cas de déni de service des systèmes globaux. Cette sous-problématique ouvre néanmoins des questionnements éthiques et juridiques, qu'il faudrait résoudre avant emploi de tels systèmes.

2.4 – Masse

En termes d'intelligence artificielle, la masse, entendue comme la capacité à générer et entretenir des volumes de force suffisants pour produire des effets de la décision stratégique dans la durée, s'oriente majoritairement vers les technologies de robotique automatisée. Grâce aux technologies d'intelligence artificielle, en particulier les réseaux neuronaux pour la simulation multi-agents, il est possible d'envisager ce que Paul Scharre

[21] https://www.darpa.mil/news-events/2013-04-30

[22] Par un système de traitement agile en inférence bayésienne par exemple.

[23] J-P. Baulon, « Les trois guerres de Robert McNamara au Viet-nam (1961 – 1968) et les errements de la raison dans un conflit irrégulier », *Stratégique*, 2009/1 (N° 93-94-95-96), pp. 425-444.

nomme le *Centaur Warfighting*[24], à savoir la combinaison des machines et des humains pour atteindre les objectifs assignés aux forces. En ce sens l'idée d'une robotique collaborative agissant en essaim, applicable à de nombreuses fonctions, se révèle particulièrement pertinente. Il est ainsi possible d'envisager l'accompagnement du groupe de combat par des drones – équipés de capteurs ou d'effecteurs – suiveurs ou éclaireurs, destinés à augmenter ses capacités, à l'image d'un ou plusieurs drones aériens automatisés pour une cartographie urbaine en temps réel ou des relais de communication dans des environnements contestés en termes électromagnétiques, ou détecter les pièges voire leurrer l'adversaire. L'entreprise *Swarm Systems* a effectué en 2008 une démonstration pour le MoD britannique d'un tel dispositif[25], même si de nombreuses améliorations demeurent nécessaires dans le comportement en essaim des drones. Les essaims de drones terrestres ou aériens *low cost* entraîneraient ainsi une saturation des capteurs de systèmes de défense adverses[26]. Ils faciliteraient des concentrations rapides dynamisant la manœuvre classique et apportant l'incertitude sur la position réelle des combattants au sein du dispositif d'hommes et de machines augmentant ainsi la résilience globale et préservant les hommes. La masse impliquerait dans ce cas également, une optique de sacrifice potentiel permettant d'épargner la vie des combattants.

Même en dehors des essaims de drones, le concept de *combat centaurique* peut trouver une application dans des domaines très spécialisés, par l'utilisation de cobots directement emportés par les humains ou non. La fonction NEDEX par exemple représente un cas particulièrement pertinent de collaboration potentielle robot-automatisé/humain, afin de préserver la vie des combattants, notamment dans des environnements pollués par des EEI. Le domaine terre qui comprend également des actions sur les espaces aériens, électromagnétiques voire maritimes, dispose de nombreuses potentialités d'applications, par les avancées réalisées ces dernières années dans la robotique terrestre automatisée[27].

2.5 – Endurance

L'endurance – comme capacité à durer et à supporter l'enchaînement des opérations – reste un défi pour les forces armées contemporaines, confrontées à l'élongation logistique et à la complexification technique des matériels. En 2009, un rapport de Deloitte sur l'action américaine en Afghanistan pointait le taux très élevé de pertes le long de la

[24] P. Scharre, *op. cit.*

[25] https://webarchive.nationalarchives.gov.uk/20140410093216/http://www.science.mod.uk/Codex/documents/Codex_issue2_GC_Supplement.pdf

[26] Le programme de drones en essaims LOCUST conduit par Raytheon pour l'US Navy vise précisément cet objectif : https://www.defenceprocurementinternational.com/features/air/drone-swarms

[27] En regard notamment du déploiement de robots terrestres (Uran-9, Taifun-M) par les forces russes en Syrie, même si le caractère plus ou moins « automatisé » de ces derniers demeure encore à démontrer.

chaîne logistique pétrolière des forces, signe de l'importance de celle-ci, aussi bien que de sa vulnérabilité[28]. L'intelligence artificielle, dans ce contexte, dispose de plusieurs applications possibles que ce soit en tant que système centralisé de gestion des parcs, ou en tant que système embarqué sur des véhicules autonomes.

2.5.1 – *Action sur le système logistique/MCO par une vision prédictive*

L'IA, par la capacité d'agencer et de traiter des informations issues de capteurs multiples sur des véhicules et matériels, permettrait de modifier le paradigme du MCO d'une vision curative par parc entier, vers une vision prédictive par équipement individuel. En anticipant les ruptures de pièces ou de sous-systèmes, il est possible d'envisager un MCO du champ de bataille extrêmement réactif[29]. Les principales entreprises de défense et d'aéronautique à l'échelle mondiale travaillent sur des offres liées à du MCO prédictif des matériels, à l'image de Boeing associé à l'entreprise *SparkCognition*[30]. De nombreuses solutions d'IA disponibles dans le domaine civil, comme Watson d'IBM, sont d'ores et déjà utilisées dans ce domaine, et des applications duales pourraient être envisagées pour l'armée de Terre, en parallèle d'une augmentation des capteurs sur les équipements[31].

2.5.2 – *Robotisation d'un certain nombre de fonctions*

La robotisation d'un certain nombre de ces fonctions peut également être envisagée, à l'image des projets conduits par la firme israélienne IAI, dans le domaine des drones terrestres autonomes. Les projets RoboCon pour les convois logistiques autonomes[32] et REX pour l'accompagnement des groupes de combat[33] démontrent une certaine avance dans ce domaine et une préoccupation majeure des forces israéliennes. Toutefois plusieurs problèmes se posent dans ce cas : d'une part l'absence de discrétion comme démontré par le rejet de l'US Marine Corps du robot LS3 de Boston Dynamics, considéré comme trop bruyant[34] et, d'autre part, la difficulté à considérer une robotique automatisée dans des environnements non balisés comme le désert.

Il est également possible d'examiner l'utilisation de systèmes robotisés pour combattre dans les zones polluées, soit par les conséquences des combats, soit par l'utilisation

---

[28] C. Wald et T. Captain, *Energy Security, America's Best Defense,* Washington, Deloitte, 2009.

[29] Lequel peut être complété par d'autres technologies comme l'impression 3D.

[30] https://www.mro-network.com/technology/nothing-artificial-about-how-ai-transforming-mro

[31] En prenant en compte les externalités négatives de ces derniers comme la consommation énergétique accrue.

[32] http://www.iai.co.il/2013/37135-48072-en/Business_Areas_Land.aspx

[33] http://www.iai.co.il/2013/37135-40068-en/Business_Areas_Land.aspx

[34] https://www.theguardian.com/technology/2015/dec/30/us-marines-reject-bigdog-robot-boston-dynamics-ls3-too-noisy

d'armements chimiques biologiques ou nucléaires. Le retour des rhétoriques sur l'emploi des armes nucléaires tactiques – avant tout dans une optique d'escalader pour désescalader – peut en effet se traduire par la volonté de créer des environnements inhabitables, en effectuant une sorte de contre-mobilité à moyenne échelle. Dans ce contexte, cette capacité d'exploiter des compartiments de terrain invivables doit être considérée soit pour nos propres forces, soit à craindre de la part de l'adversaire, surtout si ce dernier se montre capable d'exploiter les synergies entre armes de destruction massives et robotique[35].

2.6 – *Force morale*

Les systèmes IA existant dès à présent dans le domaine médical civil pourraient être utilisés par l'armée de Terre dans la gestion de l'état psychique des combattants et des commandants. Par l'intromission de multiples capteurs dans les équipements des combattants, destinés à enregistrer et à analyser plusieurs paramètres biologiques (rythme cardiaque, encéphalogramme, etc.) d'une manière non-invasive, les spécialistes infirmiers et médicaux disposeraient de multiples données sur l'état des combattants. L'IA serait en ce sens envisagée comme un soutien pour le pré-traitement de ces données, en établissant des corrélations de données médicales en temps réel – voire prédictives – sur l'état de tel ou tel soldat et sur la possibilité de contracter une pathologie spécifique (ex : PTSD). Il ne s'agirait pas en ce sens d'augmenter la force morale, mais bien de contrôler l'état de celle-ci, tout en prévenant les risques de rupture psychique.

Le traitement de données médicales multiples par des agents intelligents est non seulement une technologie relativement mature, mais fait également partie des préconisations du rapport Villani en ce qui concerne les priorités de développement de l'IA en France.

De la même manière, les technologies de communication Homme-Machine pourraient inclure des interfaces modulables capables d'adapter leurs messages à la situation psychique des individus utilisant les machines.

2.7 – *Influence*

L'influence qui consiste à « agir sur les perceptions à un degré équivalent aux actions cinétiques et classiques », implique dans ce cas, un traitement de nombreuses variables environnementales afin d'obtenir un effet positif sur la population[36]. Dans le cas d'un

[35] Il est à ce titre intéressant de considérer les efforts de la Russie sur le segment de la robotique terrestre, automatisée ou non.

[36] Cette sous-partie ne traite que de l'influence positive officiellement conduite par l'armée de Terre. L'influence négative (*black psyops*) qui est du domaine des actions spéciales ou clandestines, n'est pas comprise dans cette étude.

environnement multifactoriel complexe, l'Intelligence artificielle peut avoir de nombreuses applications au service des actions d'influence entreprises par une force sur le théâtre. La capacité de l'IA d'apprentissage de langages – au travers de systèmes traitant du *natural langage processing* – peut permettre une élaboration extrêmement fine des *master messages,* à diffuser auprès des acteurs locaux que l'armée de Terre côtoie. De la même manière, l'IA peut faciliter l'identification des profils de type *key leader* et la compréhension des organisations humaines pour mettre en œuvre les opérations d'influence de la manière la plus fine possible.

Il s'agit également de réagir aux manœuvres d'influence adverses. Si la détection de celles-ci est d'avantage du ressort du FSO « compréhension »[37], l'élaboration de messages dynamiques destinés à contrer celles-ci peut être confiée à un système automatisé travaillant à partir d'une base de données extensive de type *big data*.

L'incorporation de l'ensemble de ces éléments pourrait s'opérer au niveau du commandement de la force sur théâtre (type PCIAT) voire même demeurer sur le territoire national au niveau du CIAE. En effet, la nature particulière du cyberespace, sous-tendant le système mondial de communications, n'impose pas une présence de ce type d'outil destiné à l'identification et à l'élaboration de messages, au plus près du terrain. De même, les outils considérés pour ce type d'application spécifique peuvent être dérivés d'applications civiles comme celles dédiées au marketing ciblé, à l'image de *RankBrain* développé par Google à partir de l'outil IA open source *TensorFlow*[38].

De fait sur cet usage, l'armée de Terre se différencie peu de certaines autres composantes des forces armées comme le COS, mais en outre, elle ne se démarque que dans la finalité d'organisations non militaires, comme les entreprises ou les ONG. L'usage de technologies civiles peut ainsi se révéler parfaitement adapté dans le contexte plus global des systèmes dédiés au neuro-marketing[39].

2.8 – Performance du commandement

En ce domaine, l'IA peut s'envisager comme une aide précieuse à la prise de décision. Le transfert, dans le domaine du commandement, des systèmes experts qui ont fait leurs preuves dans le domaine médical comme aide au diagnostic, pourrait se révéler alors un atout important dans la décision tactique, surtout si ces derniers sont en mesure d'intégrer une fusion de données de natures hétérogènes.

---

[37] Par l'usage entre autres de *bots* d'analyse de type *web crawler* détectant des schémas communicationnels sur les médias identifiés, tels les réseaux sociaux.

[38] https://www.tensorflow.org/

[39] Voir à ce sujet les travaux de D. Kahneman (*Choices, Values and Frames* (avec A. Tversky), Cambridge, CUP, 2000) ou ceux de C. Schmidt (*Neuroéconomie. Comment les neurosciences transforment l'analyse économique*, Paris, Odile Jacob, 2009).

Ce type de système, qu'il soit une déclinaison militaire d'un système préexistant dans le civil ou une création dédiée, ne présente que peu de spécificités pour l'armée de Terre, en regard des autres armées. Il y a donc un véritable intérêt à la mutualisation au sein des Armées, voire au sein de l'OTAN, pour des questions d'interopérabilité au niveau des systèmes C4ISR.

FSO	Application	Spécificité Terre
Compréhension	+++	Partielle (environnement humain)
Coopération	++	Non
Agilité	+	Non
Masse	++	Oui
Endurance	++	Oui ; usage de technologies duales possible
Force morale	+	Non ; usage de technologies duales possible
Influence	++	Partielle ; usage de technologies duales possible
Performance du commandement	+	Non ; usage de technologies duales possible

3 – Vulnérabilités à 2035 de l'armée de Terre face à l'IA

3.1 – Combattre un adversaire partiellement ou totalement doté d'IA/robots

La problématique de l'IA au sein de l'armée de Terre doit également prendre en compte les nécessités du combat contre des adversaires dotés de ce même type d'équipement. Sans entrer dans les différents modes d'action qui pourraient être employés dans ce contexte, il est toutefois nécessaire de prendre en compte certains éléments.

Le premier d'entre eux est le développement des IA dans un certain nombre de forces armées. Les États-Unis et la Chine qui sont en tête de ces programmes d'IA militaires, ont été rejoints par de nombreux pays comme Israël ou la Russie, avec un prisme particulier sur la robotique terrestre autonome dans ces deux cas. Il faut cependant envisager,

après le déploiement au sein de leurs propres forces, de voir des produits militaires intégrant des systèmes IA proposés à la vente. Dans le cas d'un conflit de haute intensité entre acteurs étatiques à l'horizon 2035, la probabilité pour l'armée de Terre de faire face à des systèmes intégrant de l'intelligence artificielle reste relativement importante.

De manière tout aussi importante, il devient nécessaire d'appréhender la possibilité de rencontrer vers 2035, des adversaires non-étatiques disposant de capacités IA limitées, mais permettant une supériorité locale temporaire. La multiplication des logiciels de *machine learning* en *open source*, comme *Google TensorFlow* par exemple ou *Torch*[40], permettra ainsi de disposer d'outils de programmation de plus en plus puissants. Cette facilité d'accès aux logiciels qui se combine à la capacité actuelle de détournement d'un certain nombre de robots commerciaux (comme des UAV de loisir) de leur usage, pourrait donner un avantage non-négligeable à des groupes armés terroristes dans le futur. Daech par exemple a montré son inventivité en Syrie et en Irak pour créer des drones armés à partir de simples systèmes commerciaux. La disponibilité des robots commerciaux, des logiciels de programmation *open source,* mais également des capteurs optiques ou électromagnétiques de bon niveau – sans parler des images satellitaires commerciales –, donnera à une force légère et inventive, des capacités accrues en termes de renseignement et de conduite des opérations.

L'armée de Terre doit donc se préparer, dans un scénario maximaliste de développement de l'IA, à faire face à des adversaires étatiques ou non, disposant de capacités augmentées par l'apport de l'intelligence artificielle. La vulnérabilité du système Scorpion, notamment la vétronique des véhicules et les systèmes d'info-partage, doit ainsi être considérée, au prisme de cette possibilité d'une capacité adverse – temporaire ou permanente –, d'utilisation de systèmes IA à des fins offensives.

3.2 – Vulnérabilités intrinsèques du développement de l'IA dans l'armée de Terre

3.2.1 – Facteurs industriels

Concernant une nouvelle technologie comme l'intelligence artificielle, la première des vulnérabilités tient à la disponibilité industrielle. En effet les acteurs de l'intelligence artificielle ne sont pas ou peu, du moins en France, liés au secteur de la défense. La réticence d'un grand nombre de ces acteurs – notamment des *start-up* innovantes – à s'engager dans des applications à destination des Armées pourrait représenter un frein certain au développement de systèmes au sein de l'armée de Terre, à l'exemple de ce qui peut se passer aux États-Unis, avec la crainte que ces éléments ne débouchent sur des armes autonomes ou une IA générale. En outre, l'organisation du secteur industriel de l'IA est

[40] Des exemples de solutions populaires : https://opensource.com/article/18/5/top-8-open-source-ai-technologies-machine-learning

encore balbutiante en France, suivant le rapport Villani. Il en résulte pour le moment, un recours nécessaire à des solutions étrangères extra-européennes, majoritairement américaines comme *Tensor Flow*, qui pourraient constituer des risques sur la disponibilité ou l'adéquation des IA proposées sur le marché. Une vigilance particulière doit ainsi être observée quant à l'évolution de l'écosystème de l'IA en France, particulièrement en ce qui concerne la BITD[41].

Le facteur MCO – surtout dans le cas des systèmes robotisés – est ici prépondérant. Au-delà de toute problématique classique en termes de MCO militaire – disponibilité des pièces détachées, rapidité d'intervention, etc. – le cas des IA se singularise par la question de la gestion des données d'entraînement et la mise à jour des algorithmes de traitement. Au cas où l'armée de Terre ne disposerait pas en propre de capacités dédiées à la certification, à la mise à jour des algorithmes ou à la gestion des jeux de données dédiés aux IA, ces fonctions seraient mécaniquement transférées aux industriels. Cette situation ouvrirait ainsi des risques quant à la disponibilité et à la pérennité des systèmes, sans parler des problématiques liées à la sécurité des données, s'agissant des questions liées aux entraînements.

En cas de problèmes avec une entreprise responsable du développement et de la mise à jour d'un tel système, il semble difficile d'envisager l'ensemble des conséquences, pouvant aller jusqu'à l'impossibilité d'utiliser le système IA. Les problèmes que le DoD américain rencontre en ce moment, avec certains de ses fournisseurs IA comme Google[42], toujours réticent à s'engager dans la voie des systèmes militaires, sont représentatifs du risque industriel lié à l'IA militaire.

3.2.2 – Facteurs logistiques et communication

Les systèmes d'intelligence artificielle, robotisés ou non, ne peuvent être pensés en dehors d'une chaîne logistique complexe qui est une extension globale de la chaîne logistique des systèmes C4ISR. En effet, en tant que système informatique, fixe ou mobile, le système IA reste soumis à différents impondérables parmi lesquels l'alimentation en énergie, et les systèmes de communication demeurent les plus importants et les plus critiques, en termes de protection.

Les systèmes IA sont ainsi, comme tout système informatique, extrêmement dépendants des approvisionnements électriques pour fonctionner. Il en ressort pour les IA déployées sur les théâtres d'intervention, la nécessité de penser encore davantage la robustesse et la résilience des systèmes énergétiques militaires. Au-delà de cette question

[41] Voir infra.

[42] https://www.theverge.com/2018/6/1/17418406/google-maven-drone-imagery-ai-contract-expire

– importante mais pour laquelle il existe des solutions en expérimentation[43] – au niveau des postes de commandement, la problématique de l'approvisionnement énergétique des IA embarquées sur véhicules – habités ou non – se pose avec une acuité bien plus importante. En effet, au-delà de l'énergie nécessaire pour le fonctionnement du système, émerge la question de la dépense énergétique pour les communications entre le véhicule et sa base. Plus le système a besoin de communiquer des données complexes – images, vidéos, etc. – plus la dépense énergétique devient importante. Dans le cas d'un système fortement automatisé, cette dépense énergétique de communication s'avère encore plus critique, mettant l'accent sur une externalité négative de ce type de système[44].

Il en résulte également la nécessité de disposer d'une capacité de protection des communications – principalement non-filaires – très importante. Le cryptage des communications homme-machine et machine-machine doit ainsi être pris en compte de manière décisive pour éviter les attaques cyber du type *man-in-the-middle* qui, non spécifiques aux IA[45], sont ici particulièrement dangereuses si l'on envisage celles-ci comme injection de données erronées[46]. La robustesse des communications est ici centrale, à moins de n'envisager que des systèmes disposant d'une autonomie d'action étendue, ce qui soulève d'autres problèmes d'ordre éthique ou juridique.

3.2.3 – RH et data

L'une des principales difficultés à laquelle l'armée de Terre sera confrontée en termes de déploiement de l'IA, sera liée à la disponibilité des données pour l'entraînement du système. En corollaire de cette vulnérabilité, se trouve celle concernant les questions RH avec un besoin avéré de spécialistes, que ce soit en algorithmie pour la programmation des IA elles-mêmes, en robotique pour leur intégration, mais également en management de l'information (*data scientists, knowledge managers,* etc.), pour leur entraînement et mise à jour. La combinaison de ces deux facteurs de risque, s'ils étaient réalisés, conduirait à une dépendance forte de l'armée de Terre à des prestataires externes, avec la nécessité pour celle-ci de transférer au(x) prestataire(s) des données potentiellement très sensibles.

---

[43] Voir à ce sujet les travaux menés par l'ENSEC-COE : https://www.enseccoe.org/en/newsroom/nato-ensec-coe-representatives-in-trident-juncture-2018-exercise-presenting-energy-efficiency-solutions/373

[44] Sur les questions de coût énergétique des communications cyber voir : IEA, *Digitalization and Energy,* Paris, OCDE, 2017.

[45] Plusieurs exemples de ce type d'attaque ont été répertoriés sur des drones américains dans les années 2000 et 2010 ; voir : F-B Huyghe, O. Kempf et N. Mazzucchi, *Gagner les cyberconflits,* Paris, Economica, 2015.

[46] Voir infra 3.2.3.

A.– Leurrage d'IA par injection de fausses informations

Les systèmes IA sont eux-mêmes vulnérables à certaines attaques spécifiques qui pourraient limiter leur usage dans le domaine militaire. En effet, les systèmes fondés sur la reconnaissance d'objets ou d'infrastructures travaillent suivant l'entraînement qui leur a été donné, lui-même issu le plus souvent d'une variation de l'entraînement humain, avec de multiples répétitions (apprentissage par renforcement). Toutefois la qualité des données d'entrée se révèle, dans ce cas, extrêmement élevée, puisque les systèmes IA destinés au monde militaire seront avant tout des systèmes experts mono-tâches – surtout dans les fonctions renseignement-ciblage – avec une capacité limitée de discernement.

Les technologies de leurrage d'IA (*AI spoofing*) font d'ores et déjà l'objet de publications académiques. Celles-ci s'appliquent à deux niveaux : lors de l'entraînement pour aboutir à une mauvaise reconnaissance, ou lors de l'exécution pour empêcher la reconnaissance de la bonne forme. Au niveau de l'entraînement, les techniques de leurrage d'IA fonctionnent particulièrement bien sur les IA en apprentissage profond non-supervisé[47], lorsque les IA ont tendance à créer des langages propres de fonctionnement. De même, le niveau de profondeur de travail de l'IA dans la reconnaissance d'images ou de sons peut être détourné par des attaquants. En ne modifiant que des éléments qui sont invisibles ou inaudibles à l'humain, il est possible de leurrer les systèmes de reconnaissance fondés sur l'IA comme le démontrent de nombreux exemples[48]. Grâce à ces techniques, informatiques ou non, il devient possible d'augmenter sensiblement le nombre de faux positifs et de faux négatifs dans l'identification. Il est ainsi possible d'imaginer dès à présent que les principales puissances travaillant dans le domaine de l'IA (États-Unis, Chine, Israël, Russie) développent concomitamment à leurs systèmes des contre-IA fondés sur les mêmes logiques. La principale problématique ici demeure – outre la qualité des architecture fictives mises en place par les attaquants – le niveau d'entraînement des IA et, par ricochet, les systèmes de données servant à les entraîner.

B.– Disponibilité des données trop faible

L'un des principaux risques pour l'entraînement des IA concerne la disponibilité des données. Différents tests conduits sur des IA non-militaires – comme l'exemple Tay de Microsoft – ont démontré l'importance de la qualité et de la variété des jeux de données dans le résultat final de performance des systèmes. Dans le contexte d'une organisation militaire comme l'armée de Terre, cet élément se révèle d'autant plus important que la marge d'erreur tolérée reste faible, celle-ci variant néanmoins selon le domaine dans lequel l'IA est déployée. La catégorisation des données, leur volume et leur variété – autant d'éléments primordiaux pour disposer d'une capacité d'entraînement optimale –

[47] https://www.technologyreview.com/s/533596/smart-software-can-be-tricked-into-seeing-what-isnt-there/

[48] https://www.technologyreview.com/s/601955/machine-visions-achilles-heel-revealed-by-google-brain-researchers/ ou https://arxiv.org/pdf/1801.01944.pdf

se heurtent toutefois aux nécessités de protection de ces données dans le monde militaire et, plus généralement, à la problématique de management de ces mêmes données. Les trois critères centraux du management de l'information – à savoir l'intégrité, la confidentialité et la disponibilité – doivent être étendus à l'ensemble des données « utiles » pour l'entraînement des intelligences artificielles, avec une discrimination extrêmement fine de leur niveau de confidentialité. En 2017, Eric Schmidt, CEO de Google et le directeur du *Defense Innovation Board* du DoD, mettait en garde contre la mauvaise gestion des données au sein des Armées, et les impacts de celle-ci sur le développement des systèmes intelligents[49].

Il en résulte des efforts essentiels à conduire dans le domaine du management de l'information et du RETEX. C'est en grande partie grâce à la fonction RETEX, que ce soit sur les procédures utilisées au sein de l'armée de Terre (doctrine), sur les engagements passés ou les procédures et matériels utilisés par les adversaires potentiels, que les différents systèmes seront performants ou non. Davantage que les algorithmes eux-mêmes, ce sont bien les données qui restent le matériau central de l'emploi des IA dans le monde militaire.

3.2.4 – Facteurs éthiques et légaux

De nombreux facteurs éthiques et juridiques sont soulevés par l'application de l'IA dans le domaine militaire, ainsi que dans d'autres domaines de la vie courante[50]. Dans le domaine militaire, le droit de la guerre et ses principes viennent mécaniquement limiter l'application de l'IA sur le champ de bataille. Toutefois la question de l'existence des armes autonomes, et du comportement à adopter vis-à-vis de celles-ci, demeure ouverte au niveau juridique international. Il s'agit ici non seulement d'une question éthique liée à la délégation à une machine de la décision d'employer la force contre des humains – y compris de manière graduée, sans un recours nécessaire à la force létale –, mais également d'une question juridique sur la responsabilité éventuelle en cas d'erreur d'appréciation. La possibilité de poursuivre « l'auteur » étant nulle, vers qui se retourner : l'organisme militaire employant une IA, le concepteur de celle-ci, le certificateur, etc. En l'état – en l'absence de cas concret – les instances internationales considèrent toujours ce cas sous un angle théorique, avec de multiples affrontements en termes de doctrine. Il est toutefois possible, selon les avancées du droit et l'importance du *lobbying* de tel ou tel, de voir apparaître une législation internationale plus ou moins souple à l'encontre de l'IA, dans le domaine militaire[51].

---

[49] https://www.defensenews.com/pentagon/2017/04/06/pentagon-tech-advisers-target-how-the-military-digests-data/

[50] Par exemple le droit de ne pas subir une décision juridique qui soit exclusivement fondée sur le traitement d'agents automatiques comme le prévoit l'article 10 de la Loi informatique et libertés de janvier 1978 ; voir : http://www.conseil-etat.fr/Actualites/Discours-Interventions/La-justice-predictive

[51] P. Scharre, *op. cit*.

▶ Croisement de ces facteurs avec des questions techniques

Le croisement des questions éthiques et juridiques sur l'emploi de systèmes automatisés, voire autonomes, avec des questions d'ordre technique aboutit à des réflexions importantes concernant le déploiement des systèmes IA automatisés sur le champ de bataille. Concernant des IA embarquées dans des systèmes robotisés de type drones, il est nécessaire de prendre en compte la possibilité de voir celles-ci agir dans des environnements où l'armée de Terre ne dispose pas de la suprématie électromagnétique, que ce soit par action de l'ennemi – guerre électronique – ou par la nature de l'environnement, urbain par exemple. Dans le cas de tels environnements non permissifs, il appartient de se poser la question de la pertinence de systèmes robotisés automatisés, incapables de communiquer avec leur base arrière, alors même que ces systèmes sont conçus pour éviter d'exposer directement les êtres humains à des risques létaux importants. Cette possibilité d'un environnement non permissif en termes de communication doit ainsi être prise en compte aussi bien dans la doctrine – quel emploi des systèmes robotisés-automatisés dans ce cas ? – que dans les facteurs technologiques de développement de ces systèmes – communication de proche en proche ? suivant des protocoles dédiés ? en utilisant des technologies *blockchain* ? – pour répondre à ce défi.

4 – Impacts sur le mode de fonctionnement de l'armée de Terre

4.1 – Doctrine

En termes de doctrine, il existe un besoin très net d'explicitation des conditions d'emploi des systèmes automatisés et de leur degré d'autonomie. Ces conditions doivent ainsi répondre aux 3 principes du droit des conflits armés : humanité, discrimination et proportionnalité[52].

La problématique qui se pose actuellement, notamment au niveau de la Convention des Nations-Unies sur certaines armes classiques, repose en partie sur la définition des conditions d'emploi des systèmes. Un des éléments les plus importants dans ce cadre concerne le degré d'autonomie des matériels équipés de systèmes létaux ou potentiellement létaux. Cette question du degré d'autonomie des matériels – et en corolaire du contrôle des humains sur les systèmes – doit résider au cœur des réflexions doctrinales, y compris avec une différenciation entre les missions. Ainsi des missions particulièrement dan-

[52] https://www.defense.gouv.fr/sga/le-sga-en-action/droit-et-defense/droit-des-conflits-armes/droit-des-conflits-armes

gereuses pour les opérateurs humains comme la NEDEX, ou le balisage de zones contaminées et leur décontamination, pourraient être déléguées à des systèmes autonomes au nom de la préservation de la vie humaine. En application du principe d'humanité, les IA seraient tout à fait susceptibles de s'insérer dans la doctrine de l'armée de Terre quant à certaines missions, qu'elles soient dangereuses ou concourant à éviter l'emploi de la force (influence).

Au-delà, en corrélation, la question de l'emploi des systèmes militaires automatisés au milieu des populations est également ouverte. Il s'agit en effet tant d'une question en termes d'éthique et de droit, que de difficulté technique (discrimination entre combattants et non-combattants plus difficile). Si certains milieux se prêtent davantage que d'autres à l'emploi de système automatisés, comme le milieu sous-marin[53], le milieu d'intervention de l'armée de Terre oblige à prendre en compte cette question comme prioritaire. Le principe de discrimination pousse ainsi l'armée de Terre à limiter l'usage de l'IA dans un certain nombre de domaines, notamment l'usage de systèmes létaux autonomes.

Toutefois il est également important de prendre en compte au niveau doctrinal la problématique de l'autonomie potentielle des systèmes robotisés et IA comme réponse au déni d'action dans l'espace électromagnétique. Avec une perte potentielle des liaisons de communication entre les systèmes et leur centre de contrôle, il est nécessaire d'envisager que ceux-ci puissent fonctionner de manière résiliente. En ce sens la résilience, pour ne pas qu'elle devienne simplement une interruption des fonctions liées à l'intelligence artificielle, pourrait être orientée autour d'une capacité d'autonomie dont l'ampleur doit être fixée dans la doctrine.

Une réflexion profonde doit ainsi être menée suivant plusieurs paramètres juridiques et technologiques. Les niveaux d'autonomie acceptés par mission – au regard des principes juridiques sous-tendant le droit des conflits armées – doivent être intégrés directement dans la doctrine d'emploi de l'armée de Terre, afin de pouvoir orienter les projets de recherche ou les programmes industriels.

4.2 – Organisation

4.2.1 – Quel positionnement pour l'IA dans l'armée de Terre ?

Même s'ils appartiennent globalement au domaine des technologies de l'information et de la communication, les systèmes intelligents et automatisés, par leur capacité à irriguer de multiples fonctions opérationnelles et de soutien, doivent sortir du domaine SIC pro-

[53] A cause de la présence très réduite de civils.

prement dit. L'IA en tant que telle, eu égard aux développements et applications potentielles, devient une capacité transverse dont l'enjeu doit être appréhendé au niveau décisionnel le plus élevé de l'armée de Terre, y compris par les relations qu'elle impose avec la DGA et les industriels.

Au-delà des questions techniques elles-mêmes et de l'usage au sein de l'armée de Terre, il est nécessaire, en termes d'organisation, d'envisager pour l'armée de Terre, la coopération interarmées sur les questions d'intelligence artificielle. En effet de nombreux systèmes pourront se concevoir avec les autres armées, et devront s'interconnecter avec ceux-ci, dans une perspective interarmées française (*joint*), aussi bien que dans une perspective interalliée (*combined*). Il s'avère indispensable de penser l'IA au plus haut niveau de l'armée de Terre, dans la proximité immédiate du CEMAT et du MGAT. A titre de comparaison, une réflexion est menée depuis plusieurs années aux États-Unis, sur la possibilité de créer un « AI Center » interarmées, en dehors de la DARPA, pour fédérer et gérer les différentes initiatives[54].

Il appartient donc de disposer d'une chaîne de décision et de responsabilité IA qui remonte, pour les aspects juridiques, technologiques et politiques, à un bureau particulier en charge de ces questions au niveau de l'EMAT. Toutefois il appartient aussi de penser la chaîne de responsabilité IA jusqu'au théâtre lui-même.

4.2.2 – Différencier les capacités IA et robotique selon les échelons de commandement

Plusieurs éléments sont à prendre en compte en matière d'organisation de l'IA au sein de l'armée de Terre, à la fois de manière verticale selon le niveau de responsabilité, mais également de manière horizontale, selon les nécessités techniques et opérationnelles.

Les organismes spécialisés de l'armée de Terre, que ce soit dans le suivi du matériel (STAT) ou les questions informatiques et cyber (CCIAT), doivent garder une place importante dans le dispositif IA central de l'armée de Terre. La STAT en tant que lien privilégié entre l'armée de Terre et les fournisseurs industriels doit disposer des capacités liées à la gestion des demandes techniques, ainsi qu'à la certification des matériels IA ou robotisés. C'est grâce à la STAT que le lien avec les industriels français, appartenant ou non à la BITD, est devenu le plus fluide. Le CCIAT doit, quant à lui, disposer en propre des capacités liées à la programmation et à l'entraînement des IA. En tant que centre expert dans le domaine informatique, il concentrerait une grande partie des compétences liées au codage et, surtout, à la gestion des données liées aux entraînements. Le CCIAT regrouperait ainsi un noyau dur de spécialistes de la donnée, aptes à gérer

[54] Même si ce type d'organisme soulève de nombreuses critiques et réticences, notamment par la peur d'une bureaucratisation du système : https://www.c4isrnet.com/intel-geoint/2018/04/18/pentagon-developing-artificial-intelligence-center/

efficacement l'adaptation des IA ou systèmes robotisés achetés, aux exigences des métiers spécifiques, ainsi que des capacités de MCO de type NTI 2, voire 3.

Au niveau opérationnel, chaque grand commandement et unité (division et brigade), selon ses spécificités, doit disposer d'un organisme (bureau, section, etc.) dédié aux questions liées aux IA et systèmes robotisés, suivant plusieurs axes (doctrine d'emploi spécifique selon les domaines, MCO niveau NTI 2, entraînement, etc.). Enfin au niveau de chaque brigade ou GTIA, une capacité minimale de MCO dédié doit être présente, en complément de la SIMMT, afin d'agir au plus près du terrain dans l'hypothèse d'unités fortement dotées en systèmes intelligents ou en robots automatisés. A ce niveau, il faudrait ainsi disposer de capacités MCO de niveau NTI 1. Il s'agit ainsi de différencier les responsabilités, les éléments les plus complexes s'effectuant au sein des organismes centraux dédiés (STAT, CCIAT voire SIMMT) quand les niveaux de commandement les plus proches du terrain bénéficient de capacités à même d'assurer une gestion au quotidien, des matériels concernés.

4.3 – RH

La problématique RH, en ce qui concerne l'intelligence artificielle, représente un défi majeur pour les Armées. A l'image de ce qui s'est passé dans le domaine de la cyberdéfense, il faut prendre en compte tant le recrutement-formation des spécialistes de bon niveau, que leur fidélisation. Cette dernière problématique s'avère majeure, dans le sens où un *turnover* RH trop rapide sur ces spécialités empêche la constitution de corps de management intermédiaires spécialisés, possédant une expérience notable (5-10 ans), dans les Armées.

En ce qui concerne le recrutement initial de spécialistes de bon niveau, les voies d'accès actuelles – notamment la possibilité limitée d'avoir recours à des officiers commissionnés – pourraient se compléter par une approche plus flexible, notamment en termes de salaire. En effet la décorrélation entre le niveau de compétence technique et le niveau de responsabilités managériales empêche, dans le système actuel, de recruter des spécialistes de haut niveau, à des salaires compétitifs par rapport à d'autres organismes étatiques ou civils. Il serait donc opportun de mettre en place un nouveau statut RH qui se calquerait sur celui des Ingénieurs et cadres technico-commerciaux (ICT) de la DGA, avec des échelons salariaux ne reflétant pas systématiquement le niveau de commandement[55]. Leur emploi se ferait alors hors des théâtres d'opérations, que ce soit en état-major ou dans des structures spécialisées (CIAE, STAT, etc.).

[55] Le système des ICT permet ainsi à la DGA de disposer en son sein de spécialistes de très haut niveau qui ne sont pas passés par son système de formation interne ; https://www.defense.gouv.fr/dga/recrutement2/presentation-des-ict-tct-recrutement-a-partir-de-bac-2

Au sein de l'armée de Terre, il existe dès maintenant la nécessité de créer une filière d'officiers supérieurs spécialistes dans les domaines IA, *big data*, robotique, pour disposer d'un corps de management supérieur. Le meilleur cadre pour une telle spécialisation serait sans doute la création d'une sous-filière au sein de l'EMSST, à côté des domaines existants (RH-finances, renseignement-intelligence économique, etc.). Grâce à ce système, un petit nombre d'officiers supérieurs de carrière pourraient accéder à des formations de haut niveau, qui seraient ensuite mises en œuvre pour l'encadrement des groupes et unités de spécialistes IA, dans l'armée de Terre elle-même et au sein des organismes interarmées (EMA, DRM, etc.).

De la même manière, le besoin en maintenance des systèmes IA au plus près du terrain dans certains cas – notamment dans l'hypothèse de robots/drones automatisés agissant ou non en essaim – oblige à penser la mise en place d'une filière de sous-officiers spécialisés. Il s'agit ici d'être en mesure de tirer le meilleur parti des fonctionnalités des équipements, y compris dans un mode dégradé-automatisé, par une meilleure connaissance des technologies sur le champ de bataille lui-même. Les futurs chefs d'engins notamment devraient être en mesure de comprendre et d'interagir avec les systèmes IA-robotisés, particulièrement dans l'application de fonctionnalités plus ou moins automatisées. L'armée de Terre doit donc s'inspirer d'un modèle qui existe au sein des autres armées, notamment la Marine nationale, de formation spécifique tout au long de la carrière avec une montée en compétence technique par brevets. Le système des officiers mariniers avec les 3 brevets successifs (BAT, BS, BM) est un modèle possible, permettant de disposer *in fine* de sous-officiers supérieurs avec un niveau de technicien expert. Il pourrait s'agir d'un brevet spécifique de *combat infovalorisé, de « mecatronicien »* divisé en 3 niveaux correspondant à des fonctions précises[56]. Il s'agirait ainsi de valoriser les viviers de recrutement disponibles par une formation progressive sur un domaine technique, tendant à augmenter de manière graduelle les compétences des futurs encadrants immédiats du système Scorpion[57].

Cette adéquation entre des spécialistes civils de haut niveau issus des écoles dédiées (INRIA, IRT, etc.) et des personnels militaires officiers et sous-officiers donnerait à l'armée de Terre une autonomie sur la gestion de ses IA à la fois en OPEX, et hors du théâtre des opérations.

[56] Un premier niveau d'initiation pourrait ainsi permettre d'appréhender les mécanismes de gestion de l'information dans le système (chef d'équipe), un second niveau d'application serait centré sur la *data science* elle-même (chef d'engin) et un troisième niveau de maîtrise sur de l'écriture et injection de code (chef de section/adjoint chef de section).

[57] Cette formation de spécialité, complétée par des entraînements en simulation et du *drill* assisté par IA, se déroulerait à la sortie du cursus de formation traditionnel des sous-officiers de l'armée de Terre.

4.4 – Entraînement

Deux sous-problématiques se dégagent ici : d'une part l'entraînement des troupes utilisatrices de l'IA et, d'autre part, l'entraînement des IA elles-mêmes.

Concernant l'entraînement assisté par IA, le DoD américain, et plus spécifiquement la DARPA, ont mis en œuvre, ces dernières années, plusieurs programmes liés aux environnements fictifs hautement immersifs (EFHI), favorisant un réalisme extrêmement poussé. L'exemple le plus connu est celui de l'IA d'entraînement au combat aérien ALPHA, développée par une firme spécialisée pour l'*US Air Force Research Laboratory* qui, en 2016, a démontré ses capacités contre un ancien instructeur de l'US Air Force[58]. Grâce à ce type de systèmes – ALPHA est capable d'opérer sur des ordinateurs à la capacité de calcul relativement limitée – il est possible d'envisager des entraînements complexes immersifs utilisant des systèmes, de visualisation tridimensionnelle. De nombreuses entreprises américaines du monde de la défense ont déjà commencé à développer des solutions fondées sur ce type de système, pour permettre différents niveaux d'entraînement, que ce soit individuel (tir, commandement, etc.) ou collectif[59]. L'entraînement reste ainsi l'une des principales priorités d'investissement dans l'intelligence artificielle des forces armées américaines, pour les prochaines années[60].

La problématique de l'entraînement est fondamentale dans le cas des IA puisqu'il conditionne immédiatement leurs performances. De fait, la dichotomie entre les systèmes d'entraînement supervisé et non-supervisé, au-delà des enjeux qu'elle porte en termes RH sur le besoin de spécialistes, recouvre des questions de fiabilité de l'IA. Si les entraînements non-supervisés apparaissent comme offrant plus d'agilité aux IA dans le contexte d'environnements non-balisés – comme dans la majorité des théâtres d'opération – il est certain que la difficulté d'évaluation qui en résulte se montre difficilement compatible avec les usages militaires, du fait de l'usage de la force.

Au-delà de cette question du type d'entraînement, une constante se dégage : le besoin de données pour alimenter le système. Les études sur l'IA démontrent toute une corrélation forte entre la qualité et la variété des données par rapport à la performance dans les tâches demandées ensuite. Il en résulte un besoin renouvelé en termes de RETEX. Grâce aux données remontées par les RETEX de tous niveaux et par une numérisation *a priori* méticuleuse de zones futures d'opérations, l'entraînement des IA pourra se faire dans les conditions les plus proches possible de la réalité opérationnelle de l'armée de Terre, dans les spécificités du combat aéroterrestre.

---

[58] https://magazine.uc.edu/editors_picks/recent_features/alpha.html

[59] Par exemple Booz Allen Hamilton : https://www.boozallen.com/expertise/analytics/immersive-experience.html

[60] https://www.defensenews.com/intel-geoint/2018/02/16/heres-where-the-pentagon-wants-to-invest-in-artificial-intelligence-in-2019/

4.5 – Soutien

En termes de soutien, les capacités IA et robotique automatisée nécessitent une prise en compte à tous les niveaux de la chaîne par une internalisation du MCO, ainsi qu'une place prépondérante des armées dans le développement des solutions techniques.

4.5.1 – Processus de contrôle des performances des algorithmes

Le soutien des IA et des systèmes robotisés automatisés s'effectue dans une optique *bottom-up,* depuis la cellule responsable du MCO dédié sur le terrain, vers les organismes dédiés sur le territoire national (CCIAT, STAT et SIMMT), afin de prendre en compte les performances et défaillances des systèmes. Une évaluation permanente des systèmes intelligents doit être menée dans les premiers temps de leur déploiement opérationnel, et permettrait en outre de disposer d'un RETEX s'avérant idéal pour l'entraînement des autres systèmes IA.

4.5.2 – Processus de mise à jour des algorithmes

Sur le théâtre des opérations, la présence au sein des systèmes de commandement, de niveau tactique (GTIA) ou opératif, de spécialistes dédiés au MCO des IA et systèmes robotisés permettrait le contrôle de l'apprentissage en continu des systèmes, suivant leur expérience du terrain. La nécessité d'inclure aux niveaux les plus bas possibles, des sous-officiers supérieurs et des officiers formés aux domaines de l'IA, de la robotique et de la gestion des données, est un gage de la continuité dans la performance de ces matériels et systèmes. Leur compétence s'avèrerait nécessaire pour la mise en œuvre – voire la conception – de mises à jour particulières des algorithmes, afin de faire face aux menaces rencontrées.

4.6 – Equipements

La problématique des choix effectués en termes de matériels s'avère cruciale pour l'armée de Terre. Elle se comprend dans une double optique, à la fois vis-à-vis des industriels eux-mêmes, et vis-à-vis du traitement des données nécessaires aux IA.

L'évolution de la BITD qui va résulter de l'apparition de l'IA dans les programmes d'armement, doit être prise en compte. Celle-ci se fera de manière différenciée selon les scénarios d'adoption de l'IA dans le monde militaire, et les sous-domaines considérés. Ainsi dans un modèle où les principaux intégrateurs-systémiers seraient les acteurs de premier rang dans l'IA militaire – par acquisition d'entreprises spécialisées ou création d'entités dédiées –, l'armée de Terre ne changerait que peu son mode d'interaction avec les entreprises de la BITD. Au contraire, dans une optique différente qui verrait les sys-

tèmes IA militaires principalement issus de *start-up,* non issues de la BITD ou de la conversion militaire de systèmes civils, l'armée de Terre devrait agir, au travers de la STAT, comme prescripteur de la R&T dans ce domaine. Les nécessités particulières du domaine militaire – ainsi que du sous-domaine aéroterrestre – obligent l'armée de Terre à nouer des liens forts avec des sociétés liées au développement de solution IA/robotique, au besoin en créant un « club » dédié sous l'autorité de la STAT, à l'image de ce que le COS a pu faire avec le Cercle de l'arbalète[61].

En termes de plate-forme de traitement de données, l'idée d'une singularisation de l'armée de Terre semble plutôt contre-productive. Alors que l'analyse des apports de l'IA dans les FSO montre une faible spécificité des usages de l'armée de Terre et une tendance aux usages interarmées, il serait préférable, pour des raisons d'interopérabilité, de disposer d'une plate-forme commune[62]. Le projet ARTEMIS porté par la DGA[63], s'il dispose d'une orientation plutôt « air »[64], pourrait être une base intéressante de mutualisation de données interarmées destinée à alimenter les IA militaires. Il est en tout cas nécessaire que celle-ci soit située au sein du ministère des Armées, afin de ne pas laisser les industriels en charge de ce domaine. La gestion des données qui se révèle cruciale pour l'entraînement des IA, doit être à la charge des Armées, les seules habilitées à gérer le paradigme besoin de données en volume et qualité – sécurité, intégrité et disponibilité des données. En effet les spécialistes de l'apprentissage, intégrés au sein des Armées, doivent pouvoir évaluer, en permanence, les performances des IA, en corrigeant au besoin les modes d'apprentissage.

CONCLUSION

Les technologies liées à l'intelligence artificielle promettent d'ores et déjà une transformation de la guerre, eu égard au potentiel effet nivelant, sur les capacités traditionnelles. Si certains analystes américains, comme l'ancien général du corps des Marines John Allen, parlent ouvertement d'une ère de l'*hyperwar*,[65] par la combinaison des effets aux niveaux tactique, opératif et stratégique, la réalité de cette immixtion de l'IA sur et hors du champ de bataille reste à analyser. Il appartient donc, pour l'ensemble des technologies liées à l'automatisation (IA, robotique, etc.), de mener une analyse en profondeur des

[61] https://cercledelarbalete.org/

[62] Il serait ainsi important d'éviter le cloisonnement de données, comme celui-ci peut apparaître dans un domaine comme le renseignement avec l'usage de logiciels spécifiques de type SAEr-c, difficiles à faire interagir avec les systèmes de la DRM, en attendant le système SORIA.

[63] https://www.defense.gouv.fr/dga/actualite/big-data-et-ia-la-dga-presente-le-projet-artemis

[64] Ce qui est également le cas pour un autre programme DGA lié à l'IA : MMT (https://man-machine-teaming.com/axes-et-thematiques-l06-soutien/).

[65] https://fortunascorner.com/2017/07/10/on-hyper-war-by-gen-ret-john-allenusmc-amir-hussain/

opportunités de déploiement sur tel ou tel segment. L'ensemble des facteurs de supériorité opérationnelle peut ainsi être touché par ces technologies mais selon des modalités différentes, avec des spécificités particulières pour l'armée de Terre.

Si une transformation importante de certains éléments de l'armée de Terre, en particulier au niveau du cadre RH, s'avère nécessaire, l'utilisation de l'IA dans les conflits ne doit pas remettre en cause l'ensemble du mode de fonctionnement. Alors que les technologies d'intelligence artificielle s'apparentent avant tout à des cyber-prothèses pour les combattants et les décideurs militaires, elles ouvrent également des vulnérabilités nouvelles ou en augmentent certaines déjà existantes. Il importe ainsi de ne pas entrer aveuglément dans une course à la technologie trop effrénée, alors que cette dernière est déjà lancée par les plus grandes puissances militaires, pour ne pas se retrouver dans une position délicate en termes de dépendance industrielle ou de vulnérabilités opérationnelles. Il s'agit ainsi de bien distinguer les priorités de travail pour l'armée de Terre, lesquelles seraient avant tout liées à des questions organisationnelles et de soutien.

Annexe

Scénarios prospectifs

Chacun des scénarios exposés ici présente une situation différente à l'horizon 2035. Ils racontent une situation donnée en 2035 en décrivant les cheminements qui permettent d'y parvenir. Chaque scénario est mutuellement exclusif des autres et ne prétend pas être une vision d'un futur possible, sans aucune *probabilisation.*

SCÉNARIO A – DÉVELOPPEMENT LIMITÉ DE L'IA TIRÉ PAR LE CIVIL

A.– Descriptif

Le développement de l'intelligence artificielle dans la gestion des grandes infrastructures (réseaux d'eau, d'électricité, etc.), au sein des principales puissances économiques de la planète, induit un foisonnement de cette famille de technologies. Des usages récréatifs qui se multiplient, notamment pour l'amélioration des recherches sur Internet et la modélisation du comportement des consommateurs, sont portés par les GAFA(M) et leurs équivalents chinois les BATX. Dans ce contexte, les armées bénéficient d'un certain nombre de retombées technologiques liées. Des matériels civils sont ainsi militarisés dans une optique de technologie duale, notamment pour les véhicules autonomes ou les essaims de drones qui commencent par apparaître dans le secteur du divertissement (photographie, cinéma, etc.), avant d'être récupérés par les armées dans le renseignement. L'adaptation technologique de ces matériels est souvent minimale, ce qui n'est pas sans poser de problèmes en termes de cybersécurité ou de capacités[66]. De fait, les applications purement militaires sont un peu délaissées, en particulier sur des systèmes robustes destinés à être déployés sur des théâtres de conflit au plus près des forces, au profit du transfert de systèmes civils vers le militaire.

Au plan normatif, le flou demeure puisque les Nations-Unies (au travers du Groupe d'experts gouvernementaux (UN GGE) sur les développements dans le champ de l'information et des télécommunications et au travers de la Convention sur certaines armes classiques) sont incapables d'arriver à un consensus *pro* ou *contra* l'IA dans le domaine militaire. Profitant de cette zone grise, les industriels de défense incluent de plus en plus

[66] Le cas du véhicule autonome est intéressant puisque la version civile est prévue pour un usage routier exclusivement, donc la capacité à se déplacer dans un environnement extrêmement balisé et prévisible, ce qui n'est pas le cas pour un véhicule militaire destiné aux opérations.

de systèmes utilisant de l'intelligence artificielle dans leurs produits. Néanmoins, face au faible réservoir de main d'œuvre qualifiée en France – par manque de formations de haut niveau en nombre suffisant et à cause de la fuite des cerveaux vers les États-Unis et la Chine –, les intégrateurs-systémiers et les équipementiers ont recours à des *start-ups* spécialisées dont ils ont souvent du mal à garantir la pérennité économique. Ne maîtrisant que partiellement le domaine, la BITD française fait face à des stratégies de rachat des pépites IA par des fonds souverains ou de souverainetés étrangères, ce qui amène à la perte de certaines capacités de manière récurrente. Les industriels français et européens ont ainsi du mal à conserver certaines technologies de pointe mais réussissent, *nolens volens*, à se maintenir à un niveau convenable dans la compétition mondiale.

Les armées, face à cette situation, tentent d'attirer en leur sein des spécialistes civils sortant d'écoles. Face aux perspectives de carrières bien plus limitées que dans le privé, ces derniers ne restent que le temps d'un ou deux contrats (2-6 ans), ce qui ne permet pas, là non plus, de disposer d'une masse de personnels expérimentés sur le domaine. Pour y pallier, l'armée de Terre a recours à des officiers supérieurs spécialistes SIC, qu'elle envoie se former en seconde partie de carrière dans des masters spécialisés IA. Toutefois le nombre de personnels ainsi formé demeure limité, leur capacité à *manager* des personnels civils à la culture de travail différente l'est tout autant. Cette politique de formation qui ne concerne que quelques officiers par an ne s'étend pas aux autres niveaux de personnels de l'armée de Terre et, en conséquence, le MCO des systèmes IA et IA-robotisés est avant tout assuré par les industriels. Le niveau de commande des différentes forces armées européennes reste insuffisant pour créer et conserver des chaînes de pièces détachées fonctionnant en continu ou semi-continu, ce qui induit des taux de disponibilité de certains matériels robotisés assez faibles.

Il s'ensuit que les systèmes IA et robotisés sont avant tout disponibles hors du champ de bataille, que ce soit au niveau du commandement des opérations sur le théâtre, sur les systèmes de gestion des infrastructures des bases permanentes ou semi-permanentes et à Paris (CPCO). Le déploiement des IA sur le champ de bataille, s'il est envisagé et techniquement possible, se révèle complexe et coûteux, par une faible adaptation des matériels aux exigences militaires et un transfert du civil vers le militaire qui ouvre des failles techniques qu'un adversaire disposant d'un niveau de compétence moyen pourrait exploiter. Le système Scorpion, dans ce contexte, demeure limité dans son application, par une incapacité à traiter suffisamment vite les volumes de données remontés. L'infovalorisation qui existe au sein de l'armée de Terre, est ainsi plus dans *l'a priori* et *l'a posteriori* que dans le temps réel.

B.– Tendances

▶ Poursuite de la course internationale à l'IA

La course à l'IA engagée depuis plusieurs années entre la Chine et les États-Unis – où la Russie a décidé de se greffer avant tout sur le volet militaire – est au cœur de la compétition internationale entre grandes puissances. Le domaine militaire, s'il est loin d'être le seul concerné, reste l'un des principaux précurseurs technologiques, par la capacité des États à y orienter les recherches et à agir comme prescripteur.

▶ Prégnance des géants de la donnée

Dans ce scénario, les principales entreprises américaines et chinoises de la donnée, pas exclusivement dans des domaines professionnels d'ailleurs, continuent à être à la pointe de la recherche et développement en IA. De nombreuses avancées sont ainsi dues au secteur récréatif, Google permettant, avec de la recherche sémantique vocale en de multiples langues, de faire de grandes avancées sur les algorithmes de traitement du langage naturel par exemple. De même, des sociétés privées se positionnent sur le créneau du traitement automatisé d'images à partir de photos satellites civiles, ce qui permet ensuite d'importer cette technologie dans le renseignement militaire.

▶ Caractère normatif limité

L'absence d'enceinte normative désignée – à cause en partie de la multiplicité des problématiques à traiter dans cette question de l'IA dans la conflictualité – combinée à la volonté des acteurs majeurs de laisser perdurer un flou juridique et éthique sur l'utilisation des IA dans le domaine militaire, amène à une poursuite stérile des discussions internationales, telle ou telle puissance mettant son *veto* à tour de rôle sur les textes trop contraignants.

▶ Ruptures

Ce scénario essaie d'être le plus tendanciel possible, aussi il n'envisage pas de rupture majeure comme donnée d'entrée et part du principe que le passage au quantique se fait en douceur et uniformément, sans accélérer la course aux armements.

SCÉNARIO B – ACCUEIL ASSUMÉ DU NOUVEAU PARADIGME

A.– Descriptif

Les avancées technologiques des principales forces armées de la planète (États-Unis, Chine, Russie) dans le domaine de l'intelligence artificielle, avec la mise en œuvre de nouveaux matériels robotisés grandement automatisés, dans une logique de course pour des boucles réactives courtes et une compréhension fine et globale des environnements, inquiètent les décideurs politiques français et déclenchent une prise de conscience, les amenant à renverser la table en accordant la priorité numéro 1 au domaine, dans le contexte de la crainte d'apparition de conflits sous le seuil nucléaire. Les percées technologiques dans les capacités de traitement des systèmes et la sécurité des communications – tous deux grâce aux premiers systèmes quantiques opérationnels – et dans la miniaturisation des batteries sont au cœur de cette évolution des forces armées. Dans le même temps, des regains de conflits en Afrique subsaharienne ainsi qu'au Proche et Moyen-Orient obligent les armées à se déployer sur de multiples théâtres face à des adversaires de mieux en mieux équipés. Cette double situation amène les décideurs politiques, aux prises avec des contraintes budgétaires européennes, à décréter un grand plan IA et robotique pour les armées. Celui-ci s'appuie sur une combinaison de mutualisation de la R&D avec certains de nos alliés les plus proches suivant les domaines (logistique avec l'Allemagne, télécommunications avec le Royaume-Uni, etc.) et de sanctuarisation de compétences nationales.

Les entreprises de la BITD, conscientes des enjeux et des potentiels de réussite économique, créent des divisions IA et robotique en rachetant des *start-ups* spécialisées qu'elles intègrent. Grâce à ces regroupements de compétences, les intégrateurs-systémiers – qui ont parfois créé des co-entreprises pour les projets les plus lourds en investissements – peuvent proposer des offres cohérentes où les IA sont parfaitement adaptées aux usages militaires avec, en particulier, un niveau de cybersécurité fort, évoluant aisément hors de la sphère Internet. Ainsi dans chaque segment militaire apparaissent des offres spécialisées permettant de fournir aux armées des capacités nouvelles ou avec des performances accrues. L'accent est notamment mis sur le combat urbain avec le développement des actions dans des mégapoles africaines où les groupes de combat de l'armée de Terre disposent d'essaims de drones aériens autonomes réalisant, en temps réel, la cartographie des zones et des bâtiments et servant en même temps de relais de communication. L'IA est également introduite dans de nombreux matériels suivant l'évolution du rôle des armées. Les phases de stabilisation post-intervention sont ainsi maîtrisées grâce aux systèmes de reconnaissance faciale intégrés dans les équipements des patrouilles, qui signalent les profils recherchés ou au comportement suspect et permettent de personnaliser les contacts. Les équipes NEDEX bénéficient de systèmes de robotique collaborative dans leur action de lutte contre les IED, grâce aux recherches menées sur les interactions homme-machine. Les systèmes de combat proprement dits

demeurent relativement hors de ce périmètre à cause de l'impossibilité de discriminer finement les intentions et la nature des individus sur le champ de bataille. En ce domaine, les IA demeurent limitées à des systèmes d'autoprotection (anti-aérien, anti-projectiles, etc.) et à des sentinelles de garde des infrastructures militaires, sans toutefois disposer d'une autonomie d'ouverture du feu ou sans être équipées de systèmes létaux. Cependant des armements guidés par IA apparaissent dans les équipes d'opérateurs des forces spéciales. Ils utilisent des munitions particulières pour des armes de soutien spécifiques (fusils anti-matériels, lanceurs 40 mm pour grenades dronisées), dans des missions où la recherche de la précision est un facteur discriminant. Le coût unitaire de telles munitions empêche cependant leur généralisation à l'ensemble des forces.

Au niveau RH, l'armée de Terre, consciente de l'enjeu, décide de créer des filières spécialisées en son sein. Un parcours IA est proposé aux officiers réussissant le DT de l'EMSST, afin de disposer d'un vivier de spécialistes-managers du domaine. De même, en prenant exemple sur les parcours des sous-officiers supérieurs de la Marine nationale et de l'armée de l'Air, l'armée de Terre crée un brevet de maîtrise supérieure, afin de disposer de spécialistes ayant un niveau presque équivalent à celui d'un ingénieur, mais disponibles au plus près des forces. En outre, sur le modèle de la DGA, un nouveau type de contrat[67] est proposé aux civils rejoignant l'armée de Terre comme chargés de mission, avec des niveaux de rémunération variables possibles suivant les profils et l'expérience, ce qui contribue à attirer et surtout à fidéliser les meilleurs d'entre eux. Grâce à cette combinaison de filières internes et de recrutement externes, l'armée de Terre dispose d'une masse critique de spécialistes à même d'accompagner les recherches des industriels, en les orientant vers les besoins opérationnels, et de traiter directement les problèmes des IA d'application militaires. Ces personnels spécialisés sont notamment en charge de la gestion des données nécessaires aux entraînements supervisés des IA et sont également en charge de ceux-ci. Cette internalisation des compétences garantit ainsi la conservation des données sensibles au sein de l'institution elle-même, avec un recours aussi limité que possible aux industriels pour le MCO spécialisé.

L'armée de Terre évolue vers un système fonctionnant sur le mode anticipatif et programmatique, que ce soit pour les entraînements des personnels et des unités, le MCO des matériels individualisé ou la planification dynamique des opérations. Grâce aux systèmes IA fonctionnant avec des jeux de données toujours plus importants, dus à la multiplication des capteurs sur les hommes et les véhicules, le système augmente ses capacités de manière incrémentale, favorisant des gains d'efficacité militaires, mais aussi financiers.

[67] Celui-ci ressemblerait dans les niveaux de rémunération et dans la souplesse aux Ingénieurs et Cadres Technico-commerciaux (ICT).

Le revers de la médaille est la prolifération de ce type de capacités, dans un premier temps au sein d'un club de grandes puissances, puis s'étendant à d'autres pays. La popularisation des IA et des systèmes robotisés automatisés au sein des différentes forces armées de la planète permet à des groupes armés terroristes de développer des parades limitées, mais néanmoins efficaces, ponctuellement de leurrage d'IA ainsi que d'acquisition de matériels civils à l'usage détourné[68], voire de créations originales au fond des garages mais pouvant être géniales ; dans ce cadre l'IA présente un caractère de capacité nivelante. Des technologies et des stratégies de contre-IA se développent ainsi au sein des forces armées, afin d'être en mesure de réagir en cas d'agression par des acteurs de haut niveau technologique. Les recherches sur les armes à énergie dirigée sont ainsi intensifiées à l'horizon 2035.

B.– Tendances

▶ Poursuite de la course internationale à l'IA

La course à l'IA engagée depuis plusieurs années entre la Chine et les États-Unis – où la Russie a décidé de se greffer avant tout sur le volet militaire – demeure au cœur de la compétition internationale entre grandes puissances. Le domaine militaire, loin d'être le seul concerné, devient l'un des principaux précurseurs technologiques par la capacité des États à y orienter les recherches et à agir comme prescripteur. La percée technologique de l'informatique quantique ouvre des possibilités extrêmement importantes en termes de capacité de traitement de données, garantissant le fonctionnement des algorithmes extrêmement complexes.

▶ Engagements militaires multiples

La pérennité des menaces, principalement non-étatiques mais pas exclusivement, amène la France à poursuivre un effort d'engagement militaire international soutenu. Alors que nombre de partenaires, principalement européens, refusent des opérations au niveau d'intensité parfois fort, la France demeure le principal garant de la sécurité du continent sur les flancs Sud et Sud-est. Cette permanence de l'engagement, avec des volumes de forces contraints, oblige à penser des solutions, y compris technologiques, pour durer dans le temps et dans l'espace.

[68] On peut imaginer des robots automatiques d'aide à la personne détournés en robots-IED autonomes.

Ruptures – Émergence technologique militaire au sein des puissances majeures

La véritable rupture consiste en l'apparition, chez plusieurs puissances majeures, de systèmes matures combinant IA et quantique. Au-delà des IA limitées en service aujourd'hui dans certaines forces armées, des IA disposant de grandes capacités de traitement, grâce aux apports de la technologie quantique – laquelle favorise en outre une meilleure sécurisation des télécommunications – ouvrent des perspectives extrêmement intéressantes, y compris en matière de robotique automatisée.

SCÉNARIO C – ADAPTATION DE L'ARMÉE DE TERRE DANS UN CONTEXTE DE PEUR DE L'IA ET DE LA ROBOTIQUE MILITAIRE

A.– Descriptif

Les progrès observés dans le développement de l'intelligence artificielle militaire demeurent fortement limités. Suite à une action à forte résonnance médiatique, les grands leaders de la Silicon Valley réussissent à créer un mouvement général aux États-Unis, en s'alliant avec des leaders religieux et syndicaux, contre la recherche militaire en intelligence artificielle, en pointant la peur du robot « tueur » ou trop intelligent. Après avoir attiré les meilleurs scientifiques en IA, le Pentagone, DARPA en tête, se trouve privé des chercheurs les plus prometteurs. En répercussion les dirigeants politiques et militaires américains, afin de ne pas perdre la course à l'IA, décident de geler son application militaire. En agissant simultanément au niveau de l'OTAN d'une part, et de l'ONU d'autre part (avec une présence forte au sein du Groupe d'experts gouvernementaux (UN GGE), sur les développements dans le champ de l'information et des télécommunications dans un contexte de sécurité nationale, ainsi qu'au sein des discussions portant sur la Convention sur certaines armes classiques (CCAC)), les États-Unis permettent de bannir l'utilisation de l'IA dans de nombreux usages militaires. Les utilisations de systèmes autonomes – avec une absence d'humain pour la décision – pour engager le feu sont strictement interdites. La problématique éthique prend ainsi le pas sur toute considération militaire, ce qui aboutit naturellement à discréditer voire diaboliser le champ militaire dans la recherche en intelligence artificielle. En France, la CNIL vient surajouter un élément en restreignant le traitement des données personnelles par des agents automatisés, en vertu du respect de la vie privée, les armées ne réussissant pas à obtenir de dérogation sur ce point.

Constatant cette limitation, de nombreux pays, à commencer par la Russie et les pays européens, désinvestissent de l'Intelligence artificielle à des fins purement militaires puisque cette dernière risque d'être limitée à des fonctions de soutien. En conséquence, les industriels de la donnée – y compris les groupes chinois sous tutelle étatique plus ou moins forte – prennent le relais et imposent leurs solutions technologiques. Les entreprises de la BITD française, limitées par les décisions politiques au niveau supranational, choisissent de ne pas investir ce champ en propre, préférant adapter les solutions civiles à leurs matériels. Ces entreprises développent des matériels robotisés terrestres qui ne sont au fond que l'adaptation des drones aériens (RPAS) au domaine terre. Il en résulte pour les armées, la nécessité de faire appel à des technologies duales auprès d'entreprises non-spécialistes du monde militaire. Deux cas de figure se présentent alors, d'abord le recours à des entreprises françaises de type *start-up* qui n'ont le plus souvent pas l'habitude de travailler avec le monde militaire ou même l'État, et ensuite le recours aux géants de la donnée américains (Microsoft, IBM, Oracle, Cisco, etc.).

Dans les deux cas, les armées se retrouvent obligées de confier leurs données sensibles à des entreprises qui sont incapables – par manque de moyen et de sensibilisation ou par volonté – de garantir la sécurité des données qui leur sont confiées. Il en résulte de la part du ministère des Armées une restriction volontaire du transfert de données vers ces entreprises, ce qui limite mécaniquement le niveau de performance des IA militaires. Dans ce contexte, constatant la faible performance des équipements ainsi produits, les armées décident de conserver l'IA dans des fonctions très secondaires, sans réelle volonté de former des spécialistes en interne. Sans évolution RH au sein des armées, le ministère des Armées devient davantage dépendant de ses prestataires, puisqu'il est incapable de leur opposer des spécialistes militaires purs travaillant pour lui.

L'IA se retrouve donc handicapée par ces effets en cascade, et reste cantonnée à des achats de solution sur étagère, pour des usages d'automatisation de certaines tâches répétitives. Les principaux domaines d'application sont le prétraitement des données de renseignement issues des capteurs images par reconnaissance de formes, et la cybersécurité avec des systèmes d'analyse du comportement de l'utilisateur. En termes organiques, l'IA n'est qu'un sous-domaine des SIC, *in fine,* considérée comme d'un apport mineur aux opérations de l'armée de Terre. La dronisation de certaines fonctions permet l'allégement de certaines charges, notamment au plan logistique, par l'intromission de certains drones pilotés à distance, mais ne change pas fondamentalement la conduite des opérations.

B.– Tendances

▶ Prégnance des géants de la donnée

Dans ce scénario, les principales entreprises américaines de la donnée, du moins celles aux usages les plus professionnels, continuent à se maintenir à la pointe de la recherche et développement en IA. L'action des dirigeants de ces entreprises est majeure, et leur impact politique leur permet de sanctuariser le marché et, par extension, de créer des marchés captifs ou semi-captifs dans les pays de l'espace euro-atlantique, et même au-delà. Seule la Chine réussit à conserver un écosystème IA fort véritablement national.

▶ Contestation des développements militaires de l'IA

Une grande partie des chercheurs universitaires de premier plan et des dirigeants des entreprises de la *Silicon Valley* demeurent opposés aux recherches d'application militaire. Le militantisme de ces leaders d'opinion et leur impact politique leur permettent d'obtenir des engagements forts de la part des autorités américaines et, de ce fait, d'agir en cascade sur les alliés des États-Unis. La mise en avant de l'aspect éthico-juridique de la question – à l'image de la problématique des drones armés dans les années 2000, mais

de manière bien plus importante – occulte les autres aspects des questions liées à l'application de l'IA dans le domaine militaire.

▶ Ruptures – Textes majeurs adoptés au niveau supranational

La principale rupture observée dans ce scénario est l'adoption de textes majeurs au plan supranational (OTAN et ONU), sous l'impulsion des États-Unis. Contraintes sur le plan national, les autorités de Washington décident de geler les avancées des autres pays par une action internationale[69]. Ces textes et la communication politique internationale associée, reprise par des ONG antimilitaristes comme *Stop Killer Robots*, ont un effet en cascade sur l'ensemble des membres de l'ONU. Les pays européens, toujours volontaristes sur les décisions onusiennes, décident de suivre ces textes à la lettre, fortement encouragés par Washington, alors que les pays hors de l'espace euro-atlantique, pour éviter de se retrouver pointés du doigt, mettent leurs programmes en attente ou en limitent le développement. *In fine* ces textes permettent aux entreprises américaines de la donnée d'empêcher l'apparition de certains concurrents et leurs réservent *de facto,* certaines parts de marché. Interdire les machines autonomes au même titre que les armes de destruction massives a un effet limitatif mais n'empêche pas que certains États poursuivent « en sous-main » des programmes techniques à même d'empêcher certaines surprises stratégiques. De même certains États, poursuivant des travaux sur la robotique pilotée à longue distance, intègrent de plus en plus les effets potentiels d'une combinaison de cette dernière avec l'usage d'armes « polluantes », (effets chimiques, radiologiques, etc.) pour la neutralisation de certains territoires.

[69] Ce type d'action rappelle, en mode inverse, l'action des décideurs américains vis-à-vis du Protocole de Kyoto en 1997. Contraints sur le plan national par l'action des lobbies pro-pétrole qui aboutit à la résolution Byrd-Hagel du Sénat en août 1997, les négociateurs américains choisissent en décembre 1997 à Kyoto de favoriser un accord faible qui ne les engagera pas quoi qu'il en soit.