ASSEMBLEE PARLEMENTAIRE DE L'OTAN

COMMISSION DES SCIENCES ET DES TECHNOLOGIES (STC)

Sous-commission sur les tendances technologiques et la sécurité (STCTTS)

INTELLIGENCE ARTIFICIELLE : IMPACT SUR LES FORCES ARMÉES DE L'OTAN

Rapport

Matej TONIN (Slovénie)
Rapporteur

149 STCTTS 19 F rév. 1 | original : anglais | 13 octobre 2019

TABLE DES MATIÈRES

I. INTRODUCTION

1. Depuis ses débuts dans les années 1950, la discipline scientifique qu'est l'intelligence artificielle (IA) a connu des périodes d'intense activité, mais aussi deux périodes « d'hibernation » qui ont vu le rythme des progrès ralentir. Au XXIe siècle, en revanche, la recherche, le développement et l'adoption de l'IA ont enregistré une hausse remarquable et prolongée. La recherche, notamment, a commencé son essor aux alentours de 2001, tandis que l'offre de produits et de services s'est multipliée à partir du début des années 2010. En guère plus de 10 ans, l'IA est donc passée des laboratoires aux mains des consommateurs. Voici quelques exemples montrant l'ampleur de l'essor de cette technologie :

- À la fin des années 1990, les experts considéraient que les algorithmes de l'IA ne seraient pas capables de battre les champions du jeu de *Go* avant au moins un siècle. En 2016, le programme *AlphaGo* de Google a battu cinq fois de suite Lee Sedol, 18 fois champion du monde de la discipline.
- La moitié de l'ensemble des inventions d'IA ayant été enregistrées a été déposée auprès des offices de brevets entre 2013 et 2018 (OMPI, 2019).
- Entre 2016 et 2017, les investissements en capital-risque dans des start-up du domaine de l'IA ont plus que triplé à l'échelle mondiale, pour atteindre 11 milliards d'euros (CESP, 2018).
- Entre 2016 et 2026, l'impact économique global de l'IA pourrait se situer entre 1 500 et 3 000 milliards de dollars américains (Chen et al., 2016).

2. Il est clair que les technologies et les applications relatives à l'IA auront un impact considérable. Comme l'indique une étude : « Il est difficile d'imaginer un seul segment de la société qui ne sera pas transformé par l'IA dans les années à venir » (CESP, 2018). Pour l'heure, les domaines dans lesquels l'impact est le plus important sont les suivants : télécommunications, transports, sciences de la vie et médecine, appareils personnels, informatique et interaction humain-machine, banque, divertissement, sécurité, industrie et fabrication, agriculture, et enfin, réseaux sociaux et numériques (OMPI, 2019).

3. L'intelligence artificielle a également commencé à susciter des changements majeurs dans le domaine militaire et stratégique. Certains analystes estiment que l'IA « est une technologie susceptible de transformer la sécurité nationale, au même titre que les armes nucléaires, l'aéronautique, l'informatique et la biotechnologie » (Allen et Chan, 2017). Cela ouvre la voie à une potentielle révolution dans le domaine militaire et à une redéfinition de la notion même de défense (De Spiegeleire, Maas, et Sweijs, 2017). D'autres analystes restent plus prudents. Selon eux, « le fait de se focaliser sur la perspective lointaine d'un changement radical pourrait bien empêcher d'avoir une conception plus nuancée, celle de changements plus lents et plus subtils mais tout aussi importants » (Cummings et al., 2018). En revanche, presque tous les experts du secteur de la défense reconnaissent que le potentiel d'application de l'IA dans le secteur militaire est de fait « présent dans tous les domaines […] et à tous les niveaux des forces armées » (Svenmarck et al., 2018).

4. Ce rapport alimente et complète les travaux menés depuis un certain temps par la commission des sciences et des technologies (STC) sur :
a) les technologies comme sources de rupture ayant un impact important dans le domaine de la sécurité et la défense ; et

Encadré 1 : Travaux connexes de la STC

Rapports sur les technologies émergentes
- Transactions secrètes : l'usage des messageries cryptées, du dark web et des cryptomonnaies par les terroristes
- L'internet des objets : promesses et dangers d'une technologie de rupture

Rapports et résolutions sur la préservation de l'avance
- Conserver l'avance scientifique et technologique de l'OTAN et améliorer la souplesse de l'Alliance
- Préserver l'avance technologique de l'OTAN : adaptation stratégique et recherche et développement en matière de défense
- Résolution 453 de l'AP-OTAN
- Résolution 443 de l'AP-OTAN

Visites exploratoires
- San Diego et Silicon Valley
- Berlin, Magdebourg et Brême
- Singapour
- Londres et sud de l'Angleterre, Royaume Uni

b) la nécessité pour l'Alliance de conserver son avance scientifique et technologique (voir encadré 1). Il a été adopté par la commission des sciences et des technologies en 2019, lors de la 65e session annuelle de l'Assemblée parlementaire de l'OTAN à Londres (Royaume-Uni).

II. BREF APERÇU DE L'IA

5. Il n'existe pas de définition communément admise de l'IA. Pour l'essentiel, l'intelligence artificielle repose sur des algorithmes conçus spécialement pour résoudre des problèmes bien précis (Sheppard et al., 2018). Ces « algorithmes servent à collecter, compiler, organiser, traiter, analyser, transmettre et utiliser des ensembles de données de plus en plus volumineux » (IISS, 2018). L'IA est souvent comparée à l'intelligence humaine car elle cherche à reproduire la boucle de traitement de l'information du cerveau humain, à savoir : perception, cognition et action. L'IA peut donc être définie comme « la capacité d'un système informatique à exécuter des tâches qui nécessitent normalement l'intelligence humaine, comme la perception visuelle, la reconnaissance de la parole et la prise de décision » (Cummings, 2018).

6. L'IA n'est pas seulement une technologie à double usage, mais à **usages multiples** (Hoadley et Lucas, 2018). Elle n'intervient jamais seule, ce qui fait dire à certains analystes que « l'IA est plus proche de l'électricité ou du moteur à combustion » (Horowitz et al., 2018). Une conséquence directe est que les consommateurs « n'achètent » pas de l'IA ; ils achètent des produits et des services qui intègrent cette technologie, ou perfectionnent leurs systèmes existants en la dotant d'IA.

7. Les produits et les services intégrant l'IA regroupent de nombreuses disciplines comprenant les travaux d'IA du passé sur les systèmes experts, le traitement du langage humain, la représentation des connaissances, le raisonnement automatisé, la vision artificielle, la science des données et la robotique. Cela dit, le domaine dans lequel l'IA connaît depuis peu une forte expansion est l'apprentissage automatique, qui recueille quelque 60 % des investissements (Renda, 2019). Le but de l'apprentissage automatique est de permettre aux machines « d'apprendre automatiquement et de s'améliorer au fil des expériences, sans être explicitement programmées » (CRS, 2018 ; voir aussi encadré 2). Les systèmes faisant appel à l'IA recherchent et recueillent des données à l'aide desquelles ils identifient des tendances et adaptent leur comportement en s'appuyant sur des instructions propres à chaque tâche. Un exemple notable d'un impressionnant programme d'IA basé sur l'apprentissage machine est le programme d'échecs *AlphaZero* de Google : en 2017, il est passé de l'apprentissage des échecs en jouant « contre lui-même » pendant seulement quatre heures à un des meilleurs programmes d'échecs disponible sur le marché. D'autres exemples courants de ce type d'algorithmes d'apprentissage sont les systèmes qui, dans les applications de vente en ligne ou de streaming, fournissent des conseils personnalisés.

Encadré 2 :
Principales techniques d'apprentissage automatique

L'apprentissage par renforcement repose sur l'idée selon laquelle l'attribution d'une récompense permet d'obtenir un comportement optimal. La machine mémorise les types d'actions qui donnent lieu à une récompense et essaie de les reproduire.

L'apprentissage profond vise à permettre aux machines d'utiliser de très nombreuses sources de données afin d'apprendre plusieurs tâches différentes.

Les réseaux neuronaux artificiels cherchent à reproduire les réseaux neuronaux du cerveau humain en envoyant des signaux par l'intermédiaire d'un groupe de neurones interconnectés, disposés en couches.

8. Une façon plus générale d'appréhender le degré de sophistication des systèmes faisant appel à l'IA est de raisonner en termes de « niveaux » (De Spiegeleire, Maas, et Sweijs, 2017). Au niveau de l'intelligence artificielle faible, les performances de la machine sont égales ou supérieures à celles du cerveau humain pour des tâches *précises* et très personnalisées. L'intelligence artificielle générale est le niveau où les performances de la machine *équivalent* à celles du cerveau humain pour *n'importe quelle* tâche. Enfin, le niveau de superintelligence artificielle est celui où la machine *surpasse* le cerveau humain pour *n'importe quelle* tâche. Tous les systèmes actuellement

disponibles appartiennent à la catégorie de l'intelligence artificielle faible. La plupart des analystes estiment que les deux autres niveaux relèvent d'un futur lointain ou ne verront peut-être jamais le jour.

9. Une autre analyse, plus fine, du degré de sophistication de l'intelligence artificielle compare le comportement de ces systèmes avec le traitement de l'information opéré par le cerveau humain (Cummings, 2018). Les systèmes faisant appel à l'IA que l'on trouve aujourd'hui ne sont pas très performants dans des situations nouvelles ou de grande incertitude. Leurs comportements sont donc fondés majoritairement sur les compétences et les règles (voir encadré 3).

III. L'INTELLIGENCE ARTIFICIELLE DANS LES FORCES ARMÉES : OPPORTUNITÉS, DÉFIS ET INCERTITUDES

10. L'IA est déjà en train de devenir une réalité pour les armées du monde entier. Toutes les forces armées modernes réfléchissent à tout le moins aux enjeux de l'IA, y compris sur les plans éthique et juridique, et un grand nombre d'entre elles se dotent déjà de solutions concrètes intégrant cette technologie (voir aussi section IV). L'IA recèle un énorme potentiel pour le secteur de la défense, mais présente aussi tout un éventail de défis (techniques, entre autres). Qui plus est, les retombées sur le plan stratégique demeurent incertaines.

Encadré 3 :
Comportements du cerveau humain en matière de traitement de l'information (Cummings, 2018)

Comportements fondés sur les compétences : Actions qui deviennent hautement automatiques pour un cerveau humain correctement entraîné.

Comportements fondés sur les règles : Actions exécutées par le cerveau humain lorsque la situation est trop complexe pour qu'il se repose sur les compétences apprises, mais où des règles claires sont disponibles.

Raisonnement fondé sur les connaissances : Actions exécutées par le cerveau humain dans les situations où les règles disponibles ne sont pas totalement adaptées, mais où il peut s'appuyer sur les connaissances accumulées.

Comportements d'expert : Actions exécutées dans des situations de grande incertitude et/ou d'urgence, dans lesquelles le cerveau humain fait appel à toute son expertise, sa capacité de jugement et son intuition.

11. Examiner de façon approfondie l'ensemble des opportunités, des défis et des incertitudes engendrées par l'IA dépasserait le champ d'observation du présent rapport (voir aussi encadré 4). C'est pourquoi cette section privilégie l'examen de deux grandes opportunités (le soutien en matière d'information et de prise de décision, ainsi que les systèmes autonomes robotisés), des principaux défis techniques et autres (notamment le débat sur les systèmes d'armes létales autonomes), ainsi que de certaines répercussions possibles sur le plan stratégique.

A. LE SOUTIEN EN MATIÈRE D'INFORMATION ET DE PRISE DE DÉCISION

12. L'être humain évolue généralement dans un environnement où les informations disponibles sont partielles. Il arrive parfois que ces informations soient pléthoriques, mais ce n'est définitivement pas le cas dans le domaine militaire et stratégique. Les responsables politiques et militaires doivent intervenir dans le fameux « brouillard de la guerre ». Le soutien pouvant être apporté par les systèmes d'IA en matière d'information et de décision présente donc un grand intérêt pour les décideurs militaires et stratégiques. Ces systèmes peuvent accroître sensiblement la vitesse et la qualité de traitement, d'exploitation et de diffusion des informations, ainsi que du processus décisionnel des êtres humains et des machines.

13. Dans le domaine militaire, l'IA peut réduire considérablement **le délai d'analyse et d'action** des êtres humains et des machines. Les systèmes intégrant l'IA et apportant un soutien en matière d'information et de décision peuvent par exemple :

- Réduire considérablement les temps de réaction des systèmes de défense en cas d'attaque par des systèmes d'armes d'action rapide (missiles hypersoniques, cyberattaques ou armes à énergie dirigée) ;
- Fournir plus rapidement aux décideurs des informations exploitables, pouvant procurer un avantage déterminant sur les adversaires ;
- Repérer rapidement des cyberintrusions en détectant des codes malveillants évasifs ou des types de comportements suspects (plutôt que des codes particuliers) ; et
- Aider à repérer les tentatives de manipulation des citoyens menées via des campagnes de désinformation.

Encadré 4: Exemples de champs d'application de l'IA dans le domaine de la défense (liste non-exhaustive)

- Soins des blessés au combat
- C4ISR (Commandement, contrôle, communications, informatique, renseignement, surveillance et reconnaissance)
- Cybersécurité et cyberdéfense
- Guerre électronique
- Gestion des ressources humaines
- Information et aide à la décision
- Renseignement
- Logistique
- Opérations de maintien de la paix
- Systèmes robotiques autonomes
- Médias sociaux
- Formation

14. L'IA peut améliorer la **qualité de la prise de décisions**, non seulement par les machines mais aussi – et c'est peut-être le plus important – par les humains. La capacité de l'IA à filtrer l'environnement riche en informations d'aujourd'hui et à communiquer des résultats de manière convaincante est à cet égard capitale et deviendra encore plus importante. Si les ressources humaines permettent actuellement de traiter, au mieux, 20 % des informations produites aujourd'hui, ce pourcentage peut baisser jusqu'à seulement 2 % (Villani, 2018). Pour citer un officier britannique agacé, les forces armées « regorgent de capteurs, sont submergées de données et manquent cruellement de renseignements » (White, 2019). Les solutions intégrant l'IA peuvent apporter une aide, comme :

- Fournir une meilleure visualisation et interprétation des données (Killion, 2018) ;
- Extraire automatiquement des flux de données (par exemple des images satellites ou de vidéosurveillance) des informations présentant de l'intérêt pour les actions de suivi (CRS, 2018) ;
- Établir une « image globale de la situation opérationnelle » à partir d'informations provenant de sources très diverses, fournies dans des formats très différents et présentant souvent des redondances ou des lacunes (Killion, 2018) ;
- Mettre en évidence les anomalies – en vue de recherches ultérieures – en comparant les points de données avec des modèles de normalité préétablis ;
- Extraire des « signaux faibles » qui ne semblent pas préoccupants en soi mais qui peuvent être très significatifs s'ils sont combinés à d'autres données (Mercier, 2018) ;
- Suggérer un ensemble d'options possibles et décrire les effets probables de chacune d'elles (Van den Bosch et Bronkhorst, 2018) ; et
- Fournir des renseignements sur le comportement de l'adversaire grâce à des informations anticipées (Demchack, 2018).

B. LES SYSTÈMES AUTONOMES ROBOTISÉS

15. L'essor de l'IA a coïncidé en grande partie avec la prolifération rapide des systèmes autonomes robotisés qui, à eux seuls, transforment le paysage militaire et stratégique. Cela n'est guère surprenant étant donné que l'IA est la technologie de base utilisée dans ces systèmes.

16. Bien que cela commence à changer, la plupart des systèmes autonomes robotisés effectuent généralement les tâches militaires « rébarbatives, dangereuses ou sales » en complétant ou en remplaçant les opérateurs humains. Les avantages de ces systèmes sont qu'ils : réduisent le risque

d’erreur humaine due à la surcharge cognitive ou, au contraire, à « l’ennui » ; libèrent des ressources humaines pour l’exécution de tâches exigeant de plus grandes facultés cognitives ; évitent la présence de militaires dans des environnements dangereux ou hostiles (Hoadley et Lucas, 2018).

17. Les systèmes autonomes robotisés sont notamment utilisés pour la destruction d’engins explosifs, les opérations antimines en milieu terrestre ou sous-marin, les missions de sauvetage, l’appui logistique, voire les opérations de combat. L’autonomisation croissante des systèmes militaires pourrait à l’avenir avoir un impact considérable sur les structures de forces. L’intégration de systèmes autonomes robotisés dans les formations de combat permettrait par exemple de réduire sensiblement les effectifs d’une unité. L’autonomisation pourrait également transformer en profondeur les concepts opérationnels. Un très grand nombre de systèmes autonomes robotisés pourraient ainsi être utilisés pour submerger les postures de déni d’accès/interdiction de zone (Hoadley et Lucas, 2018). Au niveau stratégique, le déploiement de tels systèmes pourrait donner aux pays un net avantage militaire et changer la nature de la guerre.

18. La question de savoir comment le personnel militaire et les systèmes autonomes robotisés fonctionneront ensemble devient centrale puisque de plus en plus de systèmes de ce type sont intégrés dans les forces armées (cela s'applique également aux systèmes non-robotisés à intelligence artificielle). Les scientifiques et les ingénieurs se concentrent de plus en plus sur la collaboration humain-machine.

19. Les humains et les algorithmes d'IA ont des forces et des faiblesses différentes (Madni et Madni, 2018). Il y a des domaines où les humains sont plus performants que les machines. Dans d'autres, ce sont les machines qui sont plus performantes. Et dans d’autres encore, les humains et les machines fonctionnent tout aussi bien ou tout aussi mal. Le travail en équipe humain-machine vise donc à trouver le juste équilibre entre l'humain et la machine dans l'exécution des tâches. Dans certaines situations, l'équipe humain-machine obtiendra de meilleurs résultats si l'humain est « dans la boucle », lorsqu’une grande partie du contrôle est conservée par le personnel militaire. Les opérateurs doivent conserver un niveau de contrôle humain approprié pour toute décision impliquant un recours à la force (voir ci-dessous). Cependant, les humains peuvent très bien choisir de conserver ce contrôle aussi dans d'autres situations. Par exemple, en période de crise politique aiguë, les opérateurs voudraient probablement conserver plus de contrôle sur les véhicules aériens sans pilote à proximité de territoires hostiles. Dans d'autres situations, les opérateurs pourraient simplement choisir d'être « dans le circuit ». Par exemple, lorsque des camions télépilotés suivent un véhicule de tête habité, l'opérateur peut vouloir surveiller de près le convoi, mais n'intervenir qu'en cas de problème. Dans d'autres circonstances encore, les opérateurs peuvent décider de rester « exclus de la boucle ». Un véhicule sous-marin sans pilote, par exemple, pourrait être programmé pour explorer l'environnement océanique de façon autonome, tout en maintenant le silence radio pour éviter de se faire repérer.

20. Il n'est pas nécessaire que l'association humain-machine soit statique (Madni et Madni, 2018). Les chercheurs cherchent de plus en plus fréquemment à adapter cet équilibre de manière dynamique. Par exemple, là où les humains se retrouvent en surcharge cognitive, les machines pourraient alléger davantage la charge du soldat. Les humains peuvent alors revenir dans la boucle lorsque les machines atteignent leurs limites. Il peut s'agir de situations où il est nécessaire de traiter des données complexes non structurées, de procéder à des analyses non déterministes, ou pour des situations pour lesquelles ils n'ont pas été formés ou encore, avec des exigences physiques dépassant leurs capacités (ministère de la défense du Royaume-Uni, 2018).

21. La mise en œuvre d'une collaboration humain-machine adéquate se heurte à de nombreux obstacles. Peut-être plus important encore, les machines doivent être suffisamment fiables pour accomplir les tâches assignées et les opérateurs doivent avoir confiance en leur capacité de le faire (ministère de la défense du Royaume-Uni, 2018). Comme l'humain ne supervise plus la machine en tout temps et tous contextes, il est crucial que la machine gagne et conserve la confiance humaine (Madni et Madni, 2018). En outre, les nouveaux principes d'association humain-machine exigeront

des militaires qu'ils adaptent les concepts opérationnels, les routines de formation, les structures du personnel, les cadres organisationnels, la culture institutionnelle, et plus encore. La conception d'interfaces humain-machine appropriées, comme des interfaces de réalité augmentée, et la détermination du nombre de systèmes qu'un opérateur peut contrôler seront également cruciales. Les défis techniques sont également nombreux, par exemple pour garantir une puissance de traitement suffisante et développer un *cloud computing* opérationnel et sécurisé.

22. Plus que toute autre question morale, juridique ou éthique soulevée par l'IA, l'inquiétude suscitée par les systèmes d'armes létales autonomes (c'est-à-dire des systèmes ayant la capacité de tuer sans qu'il y ait de véritable supervision humaine - voir encadré 5) a capté une grande partie de l'attention. Au sein de la commission, cette question a souvent été abordée et discutée, notamment avec des responsables du Comité international de la Croix-Rouge, des experts indépendants et des représentants des gouvernements et de l'industrie. Cela a également été une préoccupation majeure lors de la visite de STCTTS au Royaume-Uni en juin 2019, où l'IA et les systèmes autonomes étaient en tête de l'ordre du jour.

Encadré 5 : Degrés d'autonomie

L'être humain **« fait partie de la boucle »** s'il conserve un haut degré de contrôle sur les systèmes autonomes robotisés.

L'être humain est **« dans le circuit »** lorsque le système peut exécuter des actions de façon autonome, mais que lui-même conserve la possibilité de les interrompre.

L'être humain est **« exclu de la boucle »** lorsqu'il ne peut ni confirmer une action du système, ni l'interrompre.

23. Alors qu'aucune définition précise n'a été établie, les systèmes d'armes létales autonomes ne rentrent presque sous aucune autre définition. D'autre part, aucun pays n'a fait part de son intention de développer de tels systèmes et un consensus existe bien au sein de la communauté internationale sur le fait que l'être humain doit conserver un niveau de contrôle humain approprié pour toute décision impliquant un recours à la force, bien que la teneur exacte de ce contrôle reste sujette à débat (Welsh, 2018). Cependant, certains experts doutent de la sincérité des intentions russes et chinoises.

24. Alarmés par la perspective que certains États pourraient vouloir mettre au point des systèmes d'armes létales autonomes à l'avenir, un certain nombre de groupes de la société civile, de parlementaires (y compris des membres de la commission) et d'États ont préconisé une interdiction préventive de tels systèmes. Ils estiment, entre autres arguments, que s'ils étaient créés, ces systèmes :

- constitueraient une violation des lois de l'humanité et des obligations de la conscience publique ;
- ne respecteraient pas les principes éthiques et juridiques nationaux et internationaux ;
- affaibliraient les principes de responsabilité en cas de pertes de vies humaines ;
- seraient dépourvus des spécificités de l'intervention humaine, comme la capacité de ressentir de la peine, du plaisir ou de l'empathie ;
- constitueraient un affront à la dignité humaine ; et
- abaisseraient le seuil de l'intervention militaire.

25. Il convient de noter que certains experts sont en désaccord avec un grand nombre de ces arguments. Ils estiment que correctement programmés, les systèmes autonomes pourraient en fait respecter de façon générale les principes moraux, éthiques et juridiques. Ces experts soulignent en outre les effets bénéfiques d'une suppression des émotions dans le contexte des combats.

26. En novembre 2017, un groupe d'experts gouvernementaux des Nations unies a examiné la question des systèmes d'armes létales autonomes. À ce jour, une trentaine de pays ont exprimé leur soutien à une interdiction préventive, l'Autriche étant le seul pays de l'OSCE à en faire partie (Busby et Cuthbertson, 2018). La Chine a plaidé en faveur d'une interdiction d'utiliser de tels systèmes, mais pas de leur développement ou de leur production. Cependant, certains analystes

doutent de la sincérité de la Chine. Dans une prise de position à l'ONU en 2018, la Chine a établi une « définition étrangement étroite des armes létales autonomes » (Allen, 2019). Certains pays seraient susceptibles d'interdire les systèmes sur lesquels le contrôle humain est très limité. Néanmoins, la majorité des États sont soit peu motivés, soit peu convaincus par une interdiction préventive. Ceux de la seconde catégorie considèrent souvent qu'une interdiction est prématurée et qu'une meilleure connaissance de ces systèmes est nécessaire. Pour l'heure, les pourparlers au sein du groupe de l'ONU sont en cours.

C. LES DÉFIS NON TECHNIQUES DE L'APPLICATION DE L'IA POUR LES FORCES ARMÉES

27. L'intégration des nouvelles technologies dans le domaine militaire suscite toutes sortes de défis, une question qui a d'ailleurs été examinée de façon approfondie par la commission ces dernières années dans le cadre de ses rapports, visites et autres activités. Le présent rapport se concentre sur trois de ces défis.

28. **Le défi de l'investissement** : Pour tirer parti de l'IA, les pays doivent investir suffisamment d'argent pour développer des systèmes intégrant l'IA et les adopter au sein de leurs forces armées, conformément à leurs objectifs nationaux de défense en matière d'IA. À cet égard, il n'est pas inutile de rappeler que les pays doivent redoubler d'efforts pour atteindre l'objectif de 2 % du PIB pour des dépenses de défense d'ici à 2024 et consacrer au moins 20 % de leurs dépenses totales à l'achat d'équipements et à la recherche et développement (R&D).

29. **Le défi de l'innovation** : Les forces armées doivent progresser dans l'adoption et l'intégration de technologies provenant du secteur privé non spécialisé dans la défense. À l'heure actuelle, les inventions et les innovations pouvant être sources de rupture – y compris celles fondées sur l'IA – sont de plus en plus le fait de petites entreprises à but commercial. Bien que cette question dépasse le champ d'étude du présent rapport, les obstacles sont notamment les suivants :

- Processus d'acquisition inadaptés ;
- Barrières culturelles et organisationnelles au sein des forces armées, ainsi qu'entre le secteur de la défense et le secteur civil ;
- Structures d'incitation divergentes entre le secteur de la défense et le secteur civil ; et
- Absence d'intérêt du secteur privé pour certains créneaux présentant de l'importance sur le plan militaire.

30. **Le défi de la main-d'œuvre** : Ce défi se présente dans tous les cas d'intégration des technologies numériques dans le domaine militaire. Aux niveaux national et mondial, la réserve de talents dans le domaine de l'IA est maigre. Un point très important est que le secteur public ne fait souvent pas le poids face aux grandes entreprises technologiques quand il s'agit de recruter les meilleurs scientifiques et ingénieurs en matière d'IA. Un autre défi est que, dans les forces armées, le personnel militaire doit aussi s'adapter aux nouvelles technologies par le biais de l'éducation, la formation et la réalisation d'exercices, par exemple. Par ailleurs, dans certains domaines, les systèmes intégrant l'IA peuvent effectuer les tâches du personnel et donc conduire à son éviction, ce qui peut avoir des conséquences non négligeables en termes d'évolution globale des effectifs.

D. LES DÉFIS TECHNIQUES DE L'APPLICATION DE L'IA AUX FORCES ARMÉES

31. L'intégration de l'IA dans le domaine militaire présente en outre des défis techniques communs à l'ensemble des utilisateurs de cette technologie. La plupart concernent les données disponibles pour l'IA, la quantité et la qualité de ces données étant les principaux « ingrédients » pour de bons algorithmes. Il existe à cet égard deux défis de taille.

1. La vulnérabilité de l'alimentation en données

32. Les données d'entrée sont un élément central des algorithmes de l'IA. La qualité d'un algorithme dépend, d'une part, des données d'entraînement utilisées avant son intégration dans un produit ou un service et, d'autre part, des données récupérées lors de l'utilisation de l'algorithme dans le monde réel. Cela conduit à ce que l'on appelle la **vulnérabilité de l'alimentation en données** (Osoba et Welser IV, 2017).

33. Dans la mesure où il est particulièrement difficile de recueillir des ensembles de données qui soient suffisamment volumineux et représentatifs de situations du monde réel, l'IA reproduit les distorsions présentes dans ses données d'entraînement (Osoba et Welser IV, 2017). Ainsi, l'algorithme *GloVe*, qui associe des mots présentant une similitude sémantique, a été formé à l'aide de 840 milliards d'exemples tirés du web : le constat est qu'il avait fortement tendance à reproduire les préjugés sexistes et racistes (Noël, 2018).

34. Même bien entraînés, les algorithmes peuvent être très instables. Un aspect très important – peut-être plus que tout autre – est que les systèmes intégrant l'IA sont incapables de s'adapter, ou s'adaptent mal, à de nouveaux contextes, même s'ils ont un fonctionnement très similaire au cerveau humain (Hoadley et Lucas, 2018).

35. La vulnérabilité de l'alimentation en données peut parfois être beaucoup plus grande dans le secteur de la défense. Dans certaines branches du secteur, les données sont très rares, en comparaison avec le secteur civil. Ainsi, les données dont disposent les forces aériennes sur le comportement de leur aéronef en opérations de combat sont dérisoires par rapport à la réserve de données auxquelles ont accès les compagnies aériennes privées. De surcroît, le personnel militaire doit souvent opérer dans des environnements où les données sont extrêmement réduites et les situations très incertaines, par exemple dans des contextes difficiles comme l'Afghanistan (Sheppard et al., 2018). Dans d'autres branches, cependant, les données sont parfois abondantes. Les forces armées disposent, par exemple, d'un grand nombre de données relatives au personnel, qui pourraient se prêter à des applications d'IA pour la gestion des ressources humaines (mais qui soulèvent également des questions difficiles en matière de confidentialité des données).

36. Les scientifiques s'efforcent de surmonter les vulnérabilités de l'alimentation en données par divers moyens. Une approche prometteuse repose sur des concepts d'IA plus anciens, qui sont basés sur des modèles descendants qui calquent l'intelligence humaine - plutôt que sur la disponibilité de grandes quantités de données (Wilson, Daugherty et Davenport, 2019). De plus, cette approche présente l'avantage supplémentaire d'être explicable car elle repose sur une logique claire et compréhensible (voir aussi ci-dessous).

2. Les problèmes de fiabilité

37. Si le personnel militaire est invité à adopter des systèmes intégrant l'IA, il doit pouvoir avoir l'assurance qu'ils fonctionneront comme prévu. Or, ces systèmes continuent de connaître de sérieux **problèmes de fiabilité**. Dans de nombreux cas, le niveau de confiance doit être beaucoup plus élevé dans le secteur de la défense que dans de larges franges du domaine civil. Lorsqu'un site de vente en ligne recommande des produits qui n'intéressent pas le consommateur, il n'y a pas grand préjudice. En revanche, lorsqu'un système militaire intégrant l'IA fait des erreurs, les conséquences peuvent s'avérer beaucoup plus graves, parfois même causer la perte de vies humaines.

38. À l'heure actuelle, il est encore très difficile – et parfois impossible – de déterminer si les systèmes faisant appel à l'IA tirent les bonnes conclusions, voire *comment* ils les tirent. Ces systèmes apparaissent souvent comme des « boîtes noires » aux yeux des chercheurs et des opérateurs. Il arrive que les algorithmes produisent des résultats « étranges », résolvent les problèmes en utilisant une méthode fausse ou contraire à la logique, ou même « trichent » (Sheppard et al., 2018). Le concept d'IA « explicable », ainsi que la nécessité de mettre en place

des processus de validation et de vérification spécifiques à cette technologie, sont donc devenus indispensables, comme les membres de la commission l'ont également entendu lors de leur visite au Laboratoire d'intelligence artificielle (*AI Lab*) du Royaume-Uni en juin 2019.

39. Dans la mesure où les systèmes faisant appel à l'IA sont très dépendants de l'exactitude des données, ils sont aussi très vulnérables à la manipulation des données d'entrée, notamment lors de cyberopérations. Bien que le volume des données traitées soit souvent élevé, toute modification – aussi minime qu'elle soit - d'un algorithme peut avoir des effets catastrophiques. Dans le domaine de la classification des images, par exemple, il a été prouvé que la modification d'un seul pixel pouvait suffire à tromper l'algorithme (Svenmarck et al., 2018). Le moindre changement même mineur ou non intentionnel, peut donc conduire le système à l'échec complet (Noël, 2018). Dans une étude récente, un algorithme de classification d'images a identifié de façon erronée une mitrailleuse comme étant un hélicoptère (Hoadley et Lucas, 2018). Un autre angle d'attaque est celui des données d'entraînement. Les réseaux neuronaux profonds utilisent souvent des modèles s'appuyant sur des données d'entraînement provenant de tierces parties. Ces données pourraient donc être une cible intéressante pour les adversaires (Svenmarck et al., 2018). Les systèmes intégrant l'IA peuvent être eux-mêmes la cible d'attaques : des acteurs mal intentionnés, y compris des terroristes, peuvent essayer de voler ou de dupliquer leur contenu, que ce soit pour l'intégrer dans leurs propres systèmes ou pour chercher un moyen de neutraliser ces systèmes (Hoadley et Lucas, 2018).

E. L'IMPACT POTENTIEL DE L'IA AU NIVEAU STRATÉGIQUE

40. Il est difficile de savoir si l'adoption par les forces armées de produits et de services intégrant l'IA aura des effets minimes, progressifs, voire révolutionnaires, mais le fait est que les analystes stratégiques se penchent de plus en plus sur ces questions.

41. Un certain nombre d'entre eux estiment que l'IA va révolutionner le domaine stratégique et militaire. Plusieurs arguments sont avancés. Premièrement, les capacités militaires intégrant l'IA pourraient commencer à surclasser les capacités traditionnelles du secteur de la défense. Toutes choses étant égales par ailleurs, les systèmes militaires compatibles avec l'intelligence artificielle l'emporteront vraisemblablement sur les systèmes similaires qui ne le sont pas. De plus, les systèmes de haute technologie plus traditionnels pourraient être vulnérables aux nouveaux systèmes perturbateurs à IA. L'équilibre pourrait donc pencher résolument du côté des États possédant une avance dans les systèmes militaires intégrant l'IA (Payne, 2018). Deuxièmement, dans un monde où les humains sont de plus en plus éloignés des champs de bataille grâce au grand nombre de systèmes à IA, les sociétés pourraient, avec le temps, être moins exposées aux conséquences des conflits militaires, surtout la mort et la destruction qui en résultent. Cela pourrait abaisser le seuil de la guerre (Payne, 2018). Troisièmement, l'émergence et l'adoption de nouvelles technologies militaires ont souvent, par le passé, conduit à une exacerbation de ce que l'on appelle le dilemme de la sécurité (Meserole, 2018). De même, la prolifération des systèmes militaires intégrant l'IA pourrait entraîner de l'incertitude entre adversaires potentiels et, peut-être à terme, une « course aux armements à base d'IA » généralisée. Quatrièmement, l'IA pourrait avoir des effets encore plus extrêmes sur la réflexion stratégique. Comme l'a fait remarquer un analyste : « Pour la première fois depuis le début de la révolution cognitive il y a des dizaines de milliers d'années, la stratégie humaine peut être produite par une intelligence non biologique qui n'est ni personnifiée, ni enracinée culturellement » (Payne, 2018). Ce changement, s'il se vérifie, serait plus profond que l'invention de l'arme nucléaire.

42. D'autres experts sont beaucoup plus sceptiques quant à la capacité de l'IA à provoquer des changements aussi radicaux. L'adoption de systèmes militaires intégrant l'IA pourrait être simplement « une poursuite des progrès accomplis à l'ère de l'information, à savoir une optimisation des données et de la puissance de traitement en vue d'acquérir de l'avance dans un domaine » (Sheppard et al., 2018). Dans un proche avenir, l'IA sera donc utilisée dans le domaine militaire pour faire « des choses que les êtres humains n'ont ni le temps ni la capacité de faire, ou très mal »

(Sheppard et al., 2018). Il convient de noter que, bien que peut-être pas aussi profonds que ceux précités, ces changements auraient quand même certainement un impact important sur les forces armées.

43. En fin de compte, il est trop tôt pour dire quelle sera l'incidence de l'IA sur le domaine militaire et stratégique, notamment parce que certaines décisions n'ont pas encore été prises par les États. Cela fut également le cas par le passé lorsque de nouvelles technologies sont apparues dans le domaine militaire. Pour autant, il est presque certain, compte tenu des multiples utilisations de l'IA, que son adoption aura un impact sur tout l'éventail des forces, ainsi que sur d'autres tâches du secteur de la défense.

IV. L'IA DANS LES FORCES ARMÉES : APERÇU MONDIAL

44. Pour illustrer l'intérêt croissant que suscite l'IA dans les forces armées du monde entier, cette section fournit un aperçu des principaux meneurs de cette technologie dans le secteur de la défense – au sein et à l'extérieur de l'Alliance –, ainsi que des initiatives engagées par l'OTAN.

A. LES ÉTATS-UNIS

45. En tant que numéro un mondial de l'IA, les États-Unis ont activement cherché à intégrer cette technologie dans leurs capacités militaires. Le développement d'une IA adaptée au secteur de la défense continue de représenter une bonne partie des efforts qui avaient été amorcés dans le cadre de la *Third Offset Strategy* de l'administration Obama, dont l'objectif était de préserver l'avance militaire du pays. En 2018, le département américain de la défense (DoD) a publié sa propre stratégie en matière d'IA, qui sera certainement renforcée par l'initiative nationale *American AI Initiative* lancée par l'administration Trump en février 2019.

46. Le DoD continue d'investir massivement dans des programmes et des initiatives ayant trait à l'IA. Un rapport de 2017 estimait qu'entre 2013 et 2017, 1,76 milliard de dollars américains ont été consacrés à trois postes pertinents du budget de la défense (apprentissage et renseignement ; informatique de pointe ; systèmes à base d'IA) (Govini, 2017). En 2018, l'agence pour les projets de recherche avancée de défense (DARPA) a annoncé une enveloppe supplémentaire de 2 milliards de dollars pour la période 2018-2023. En 2016, le département de la défense a créé la *Defense Innovation Unit* (DIU) pour faciliter l'intégration de la technologie du secteur privé dans le domaine de la défense. Comme l'ont appris les membres de la STC lorsqu'ils ont rencontré les responsables de la DIU en octobre 2018, l'IA est un domaine clé des activités de cette unité. En 2018, le département de la défense a également créé le *Joint Artificial Intelligence Center* (JAIC), dont la mission a été présentée par son architecte en chef lors de la visite de la commission en octobre 2018. Le JAIC a été doté d'un budget de 1,75 milliard de dollars sur six ans pour superviser et coordonner les actions du DoD en matière d'intelligence artificielle.

47. Le secteur de la défense des États-Unis participe à de nombreux projets et programmes relatifs à l'IA. En voici quelques exemples :

- Le programme **TRACE** *(Target Recognition and Adaptation in Contested Environments)* de la DARPA a produit des technologies prometteuses, comme par exemple un système de reconnaissance automatique des cibles pour aider les pilotes.
- L'armée de l'air américaine développe actuellement un système similaire, appelé ***Multi-Domain Command and Control***, dont le but est de regrouper les très nombreuses données provenant d'un large éventail de sources.
- ***Project Maven*** est un important programme de renseignement, surveillance et reconnaissance, mis sur pied avec l'aide de géants du numérique américains tels que Google, Microsoft et Amazon. Utilisant des technologies visuelles assistées par ordinateur, il permet à

des analystes de traiter jusqu'à deux ou trois fois plus de données au cours d'une même période (CRS, 2018). Le système est déjà utilisé dans les opérations de lutte contre Daech.
- L'armée de terre américaine teste actuellement l'application ***Asset Performance Management*** de la société ***Uptake*** dans le but de mettre en place une maintenance prévisionnelle sur ses véhicules de combat d'infanterie M-2 Bradley. La délégation de la STC a assisté à un exposé présenté par les dirigeants d'*Uptake* lors de sa visite dans la Silicon Valley en 2018.
- L'armée de terre travaille par ailleurs sur des **véhicules de combat de nouvelle génération** pouvant facultativement être pilotés.
- Le laboratoire de recherche de l'armée de terre américaine a mis sur pied le programme ***Skyborg*** dont le but est de former les pilotes des aéronefs à l'aide d'un système à base d'IA, qui peut par ailleurs être installé dans un aéronef sans pilote (Insinna, 2018).
- La DARPA a organisé un défi, le ***Cyber Grand Challenge***, au cours duquel des machines autonomes s'affrontaient les unes contre les autres. Chacune de ces machines avait été conçue avec des points faibles, et les participants devaient créer des algorithmes d'IA capables de repérer et de combler ces lacunes tout en attaquant leurs adversaires (Hoadley et Lucas, 2018).
- L'armée de terre des États-Unis développe actuellement un outil, baptisé **Macroscope**, qui utilise les données produites par les réseaux sociaux pour mieux comprendre ces environnements.

B. L'EUROPE

48. Les États européens et l'UE ont pris de plus en plus conscience de l'importance croissante de l'IA et de ses applications. En vérité, tous les pays membres de l'UE ainsi que la Commission européenne ont adopté des stratégies relatives à cette technologie. De nombreux pays, et l'UE elle-même, ont considérablement augmenté les investissements dans l'IA et mettent en place des structures et des entités pour gérer les opportunités et les défis qu'elle représente. Toutefois, l'Europe est confrontée à un certain nombre de défis structurels. En termes d'appareillage, les acteurs européens dépendent encore fortement des fabricants de puces américains. En outre, l'UE est confrontée à une concurrence intense de la part des États-Unis, où les salaires sont plus attrayants pour les chercheurs européens. L'Europe est également comparativement moins performante pour ce qui est de traduire la recherche en produits commerciaux. Enfin, les règles européennes relativement plus strictes en matière de sécurité des données, que la plupart des Européens affectionnent particulièrement, limitent l'accès aux banques de données (Franke, 2019). En avril 2019, un groupe d'experts de haut niveau de l'UE sur l'intelligence artificielle a présenté des lignes directrices en matière d'éthique pour une intelligence artificielle digne de confiance, afin de traiter les questions de vie privée et autres préoccupations éthiques.

49. À l'heure où l'UE renforce ses initiatives de défense – notamment avec la mise en place du Fonds européen de la défense et de la Coopération structurée permanente –, la R&D sur l'IA appliquée au secteur de la défense pourrait certainement jouer un rôle important. Or, pour l'instant, la plupart des initiatives sont conçues et mises en œuvre au niveau national ou bilatéral, le Royaume-Uni et la France occupant les places de leaders en Europe.

50. Au **Royaume-Uni**, l'État a investi 1 milliard de livres sterling pour faire du pays un leader mondial de l'IA. Voici un échantillon des projets et programmes relatifs à l'IA qui sont mis en œuvre dans le secteur de la défense britannique :

- Le ministère de la défense et l'administration centrale des communications ont signé un **partenariat en matière de défense et de sécurité** avec l'*Alan Turing Institute*, un institut spécialisé dans la science des données et l'IA. Ce partenariat est centré sur des projets à long terme, mais il fournit également une plateforme de formation pour les fonctionnaires.
- L'État a créé un **laboratoire d'IA** pour accroître les capacités nationales de défense dans le domaine de l'intelligence artificielle, de l'apprentissage automatique et de la science des

données. Ce laboratoire est spécialisé dans les véhicules autonomes, la lutte contre les opérations de désinformation et l'amélioration des cyberdéfenses.
- Le laboratoire Dstl (*Defence Science and Technology Laboratory*) a organisé plusieurs **défis, concours et marathons de programmation (ou *hackathons*)** relatifs à l'IA.
- Le Dstl a conçu un système de poursuite radar, ***Moonlight***, qui utilise l'apprentissage automatique pour actualiser de façon autonome les informations relatives aux radars ennemis. Ce système fournit en outre des indications et des avertissements aux unités déployées.
- Le projet **Nelson** de la *Royal Navy* vise à utiliser l'IA pour concevoir un « cerveau de navire » susceptible d'améliorer les processus décisionnels sur ses navires militaires. Un élément clé est la création d'une plateforme de données pour l'ensemble de la flotte, qui permet d'avoir accès à toutes les données pertinentes à partir d'interfaces faciles à utiliser.
- Le DSTL a, en collaboration avec des partenaires de l'industrie, développé **SAPIENT**, un système de capteurs autonome destiné à réduire la charge de travail des opérateurs du renseignement.
- Les **systèmes autonomes robotisés** ne cessent d'attirer des investissements. En 2018, les forces armées ont testé cinq systèmes de transport sans pilote destinés, par exemple, à acheminer des soldats sur la ligne de front.

51. La **France** a investi 1,5 milliard d'euros sur cinq ans dans la R&D consacrée à l'IA, et annoncé la création d'instituts interdisciplinaires d'intelligence artificielle qui rassembleront des chercheurs du secteur public et du secteur privé. L'État a par ailleurs reconnu les avantages de l'IA pour le domaine militaire :

- L'**agence de l'innovation de défense**, qui vient d'être créée, consacrera une part substantielle de son budget de 100 millions d'euros au financement annuel d'activités relatives à l'IA (Anderson et Townsend, 2018).
- L'État français a lancé un projet, d'une durée de trois ans, relatif à la **collaboration humain-machine** pour ses aéronefs de combat, et lui a attribué une enveloppe de 30 millions d'euros. L'accent est mis sur les capteurs intelligents/à apprentissage, les systèmes indépendants et les cockpits du futur, ainsi que l'amélioration de la collaboration humain-machine.
- Le **projet Artemis** vise à mettre au point un système d'IA utilisé pour stocker et gérer le volume énorme de données militaires collectées par la France. Le projet s'appuiera sur les travaux de start-up, de laboratoires et de petites et moyennes entreprises du secteur civil.
- Le projet **Commandement et contrôle des opérations armées** a pour but de libérer les commandants opérationnels des tâches répétitives et à faible valeur ajoutée en mettant en place des solutions fondées sur les mégadonnées, l'IA, la réalité virtuelle et d'autres technologies.
- La start-up parisienne ***Earthcube*** a mis au point un logiciel d'analyse des images satellites et a signé quatre contrats avec le ministère français de la défense.

52. L'**Allemagne** a investi 3 milliards d'euros pour la R&D consacrée à l'IA jusqu'en 2025. Le pays s'est également engagé à créer 100 postes universitaires ainsi qu'un réseau de 12 centres de recherche spécialisés dans l'IA. Le développement de l'IA et son adoption par les forces armées semblent encore limités à ce stade. Cela dit, l'Allemagne a proposé à la France un renforcement de leur coopération, notamment dans le domaine de l'IA. L'IA pourrait par exemple jouer un grand rôle dans le projet franco-allemand de système de combat aérien du futur. Ce projet devrait inclure les volets suivants : assistance d'un pilote virtuel ; génération automatique des plans de mission ; adaptation des capteurs à l'environnement ; ajustement de l'interface entre l'humain et la machine en fonction de la charge cognitive du/ de la pilote ; enfin, maintenance prévisionnelle (Pagot, 2019). En août 2018, l'Allemagne a créé une agence semblable à la DARPA qui travaillera sur les technologies de rupture dans le cyberespace. Il est clair que l'IA jouera également un rôle dans ces travaux.

C. LA CHINE

53. L'intelligence artificielle est devenue une priorité absolue pour les dirigeants chinois, tant pour des applications commerciales que militaires. Comme indiqué dans le Plan de développement de l'IA de nouvelle génération 2017, la Chine vise à devenir le leader mondial de l'IA et à développer un marché intérieur de l'IA d'une valeur de 150 milliards de dollars américains d'ici 2030. Déjà aujourd'hui, le gouvernement et l'industrie ont commencé à juger que la Chine a « en grande partie comblé l'écart avec les États-Unis en matière de R&D et des produits commerciaux en matière d'IA » (Allen, 2019). Toutefois, des lacunes importantes subsistent dans un certain nombre de domaines, par exemple les compétences, les normes techniques, les cadres et plates-formes logicielles ainsi que les semi-conducteurs (Allen, 2019). Les entreprises basées en Chine jouent déjà un rôle important dans le développement mondial des technologies d'IA. Non seulement la Chine investit chez elle, mais elle le fait également à l'étranger, ce qui attire de plus en plus l'attention des Alliés.

54. Comme l'ont souligné deux intervenants devant les membres de la commission à la session de printemps 2019, l'enchevêtrement du secteur privé avec les institutions publiques, telles que le parti-État et les forces armées, facilite considérablement l'incorporation des technologies d'IA dans le secteur de la défense, puisque la coordination descendante guide clairement les priorités de développement des entreprises. L'accent mis par le président Xi Jinping sur la « fusion militaro-civile » est susceptible de soutenir cette tendance (Sheppard et al., 2018). De plus, la Chine a été l'un des premiers pays à adopter les technologies d'IA pour les appliquer à des fins de surveillance nationale. Cela réduit les obstacles à l'adoption de systèmes à IA par les militaires (Allen, 2019). Des normes de protection de la vie privée inférieures à celles en vigueur en Amérique du Nord et en Europe, combinées à l'avantage numérique des données privées recueillies, constituent également un avantage clé pour le développement de nouveaux algorithmes d'IA.

55. Les analystes estiment que les efforts de la Chine pour intégrer l'IA dans son spectre militaire s'inspirent des développements de l'IA dans d'autres pays, notamment aux États-Unis. La Chine croit en une « révolution militaire intelligente » (ou « intelligentisation ») (De Spiegeleire, Maas et Sweijs, 2017). Le gouvernement chinois considère le potentiel perturbateur de l'IA comme une occasion de devancer les États-Unis en investissant massivement dans de nouveaux systèmes perturbateurs, plutôt que de simplement soutenir les systèmes existants (Allen, 2019). Par exemple, Pékin a mis l'accent sur le potentiel de l'IA pour tous les domaines militaires et notamment pour améliorer la prise de décision sur le champ de bataille, les cybercapacités, les missiles de croisière et les véhicules autonomes, toutes étant des technologies qui pourraient poser de grandes difficultés aux États-Unis dans le contexte d'un conflit.

D. LA RUSSIE

56. Le président Vladimir Poutine a déclaré que « l'intelligence artificielle est l'avenir […]. Quiconque occupera la première place dans ce domaine deviendra le maître du monde ». Bien que la Russie traîne encore derrière les États-Unis et la Chine, elle a montré sa volonté de rattraper ses concurrents, tout au moins dans certains domaines. Cela dit, alors que les entreprises chinoises et américaines consacrent des milliards de dollars à l'IA, le secteur privé russe n'investit que 700 millions de roubles environ par an (moins de 11 millions de dollars américains au moment de la rédaction) (Horowitz et al., 2018). De nouveaux rapports indiquent toutefois que le Fonds russe d'investissement direct aurait récemment levé 2 milliards de dollars auprès d'investisseurs étrangers pour soutenir le secteur national de l'IA (bne IntelliNews, 2019).

57. Le ministère de la défense, ainsi que certains acteurs de l'industrie de la défense, jouent un rôle prédominant au regard de l'IA. Tout d'abord, la commission de l'industrie militaire russe souhaite que 30 % de son équipement militaire soient contrôlables à distance à l'horizon 2025 (Allen et Chan, 2017). Dans le cadre de cet effort, le gouvernement russe a créé une fondation pour la recherche de pointe – le pendant russe de la DARPA –, dont le budget annuel se situe aux alentours de 4 milliards de roubles (environ 62 millions de dollars américains au moment de la rédaction).

Cette fondation s'est concentrée jusqu'ici sur les technologies imitant la pensée humaine, l'analyse des données et l'assimilation de nouvelles connaissances. Elle a également défini quatre grands axes de développement de l'IA : la reconnaissance des images, la reconnaissance de la parole, le contrôle des systèmes militaires autonomes, et enfin le soutien pendant le cycle de vie des systèmes d'armes (Bendett, 2018). La stratégie nationale de la Russie en matière d'IA devait être publiée en juin 2019. En mai 2019, le président Poutine en a présenté certaines des priorités : programmes de formation, partenariats public-privé, nouvelle législation et renforcement des atouts du pays en sciences, technologie, ingénierie et mathématiques (Bendett, 2019). Vladimir Poutine ainsi que plusieurs de ses ministres ont également laissé entendre que quelque 1,4 milliard de dollars américains pourraient être investis dans les efforts nationaux d'IA pour développer la « souveraineté technologique » de l'IA (Bendett, 2019).

58. Les industries russes intègrent l'IA dans les systèmes d'armes, en particulier les systèmes autonomes robotisés (Hoadley et Lucas, 2018). Le groupe Kalashnikov aurait mis au point un véhicule terrestre contrôlé par intelligence artificielle grâce à la technologie des réseaux neuronaux (IISS, 2018). La société KRET, spécialisée dans les technologies radio-électroniques, travaillerait sur « des systèmes sans pilote capables de prendre en toute indépendance des décisions en essaim » (IISS, 2018). Par ailleurs, l'armée de l'air russe a annoncé la conception de missiles guidés à l'aide de l'IA. Il se pourrait également, selon les analystes, que les technologies civiles sur la reconnaissance des images et de la parole – dont le développement est bien avancé en Russie – soient intégrées dans les opérations d'information russes (Bendett, 2018). Il convient toutefois de noter que les projets ambitieux de la Russie dans le domaine de l'IA pourraient être mis à mal par les problèmes structurels du pays, par exemple la faiblesse de l'industrie technologique et la baisse des budgets de la défense (Hoadley and Lucas, 2018).

E. L'OTAN

59. L'IA n'a jamais figuré à l'ordre du jour d'un sommet de l'OTAN. Néanmoins, les responsables politiques et militaires de l'Alliance ont assisté à des exposés sur cette question lorsque le Conseil de l'Atlantique Nord et le Comité militaire ont consacré leur journée informelle de 2018 aux technologies de rupture, dont l'IA. Cela dit, plusieurs entités au sein de l'OTAN ont lancé des activités relatives à l'IA ou inclus cette technologie dans leurs autres activités au cours des dernières années :

- L'**Organisation OTAN pour la science et la technologie (STO)** a consacré deux de ses trois thèmes scientifiques et technologiques à l'utilisation de l'IA et des mégadonnées pour la prise de décision et pour l'autonomie. Cette démarche, ainsi que la tenue d'une réunion de nombreux spécialistes sur le premier thème, ont entraîné une augmentation des activités relatives à l'IA dans le programme de travail collaboratif de la STO, par exemple des travaux sur le niveau de contrôle humain approprié pour toute décision impliquant un recours à la force, la cyberdéfense, ainsi que l'utilisation de l'IA dans le domaine de l'information.
- Le **Commandement allié Transformation (ACT)** organise un certain nombre d'événements consacrés aux opportunités et aux défis de l'IA, par exemple lors des forums OTAN-industrie ainsi que des conférences internationales sur le développement et l'expérimentation de concepts.
- L'**agence OTAN d'information et de communication (NCIA)** a fait de l'IA le sujet central de son colloque de 2018 sur l'assurance de l'information. En novembre 2018, la NCIA a également organisé un marathon de programmation, baptisé « *Hackathon for Good* », dont le but était de mettre au point des outils d'analyse de mégadonnées, de visualisation de données et d'apprentissage automatique pour faire face à des opérations d'information. L'IA sera également l'un des nombreux sujets à l'ordre du jour de la conférence de l'industrie NITEC19.
- Le **Groupe consultatif industriel OTAN (NIAG)** s'est lui aussi investi dans le domaine de l'IA. Il a récemment produit deux études sur le sujet : l'une sur l'utilisation par l'OTAN des mégadonnées ; l'autre sur l'impact de l'autonomie sur les plans et les opérations de l'OTAN (Blunt, Riley et Richter, 2018).

- Le **programme OTAN pour la science au service de la paix et de la sécurité** a explicitement sollicité des propositions concernant l'usage de l'IA dans la lutte contre le terrorisme dans son appel à propositions de 2017.

60. Sur le plan pratique, l'Alliance a déjà fait appel aux mégadonnées et à l'apprentissage automatique, par exemple pour éliminer les doublons ou les copies redondantes de jeux de données recueillis par sa mission en Afghanistan, ou figurant dans les fichiers journaux de détection de comportements anormaux (Street et al., 2018). Des produits et des services fondés sur l'IA ont également été utilisés lors d'un exercice de réponse en cas de catastrophe organisé en 2018 avec la Serbie, partenaire de l'OTAN.

V. REMARQUES FINALES

61. En tant que rapporteure spéciale de la STC, Leona Alleslev avait indiqué en 2018 que l'Alliance devait, au minimum, continuer de remplir deux objectifs clés pour faire en sorte que l'OTAN conserve son avance scientifique et technologique, et ces deux objectifs s'appliquent l'un et l'autre à l'IA.

62. Premièrement, les pays de l'Alliance les plus innovants dans le domaine de la défense doivent conserver leurs positions dominantes. L'Alliance doit disposer de capacités de défense des plus sophistiquées pour bénéficier d'un pouvoir de dissuasion et, en cas d'échec, permettre aux Alliés de se défendre contre les menaces. Compte tenu du potentiel que représente l'IA pour les forces armées, les pays de l'OTAN les plus avancés sur le plan scientifique et technologique – en particulier les États-Unis, le Royaume-Uni, la France et l'Allemagne – doivent investir dans la R&D consacrée à l'IA appliquée au secteur de la défense, afin de se mettre à la hauteur des découvertes qui sont faites à l'extérieur. Il est encourageant de voir qu'à l'exception peut-être de l'Allemagne, ces précurseurs au sein de l'Alliance investissent des ressources substantielles dans l'IA liée à la défense.

63. Deuxièmement, l'écart technologique qui existe entre les Alliés dans le secteur de la défense doit rester suffisamment faible pour pouvoir être comblé par une interopérabilité. Au fond, c'est la grande diversité des Alliés qui fait principalement la force de l'OTAN, mais cela se traduit aussi par de grandes disparités entre les capacités de défense. Le risque existe que les investissements massifs effectués dans l'IA par les pays de l'Alliance les plus avancés n'entraînent d'importants problèmes d'interopérabilité et une perte d'efficacité militaire globale de l'OTAN. Cela dit, la bonne nouvelle est que les initiatives en matière d'IA ne nécessitent pas toujours d'importants apports en capitaux, comme la commission a pu le constater lors de sa visite à Singapour en mai 2019. Les Alliés de petite et moyenne taille dotés de scientifiques et d'ingénieurs inventifs peuvent, s'ils le décident, jouer un très grand rôle dans le développement et l'adoption de l'IA. Cela pourrait en effet constituer une contribution très efficace des plus petits pays au partage des charges au sein de l'Alliance. Pour accroître l'interopérabilité, la coopération au sein des structures de l'OTAN a un rôle important à jouer. Ainsi, l'interopérabilité devrait être au cœur des efforts déployés par la STO, l'ACT, la NCIA, le NIAG et d'autres en matière d'IA. Les Alliés qui jouent un rôle de premier plan dans le secteur des S&T devraient encourager une architecture ouverte en matière de normes et de réglementations pour le partage et le transfert de technologies entre Alliés, qui permettrait de réduire le fossé technologique, tout en respectant les obligations nationales et la nature sensible des technologies.

64. Les forces armées alliées ne pourront, à elles seules, résoudre tous les problèmes spécifiques liés à l'IA, notamment éthiques et juridiques, qui sont décrits dans ce rapport. Une impulsion beaucoup plus large devra provenir de l'ensemble de l'écosystème de l'IA. Cela dit, les États, l'OTAN et l'UE peuvent et doivent jouer un rôle essentiel pour surmonter les difficultés que suppose l'adoption de l'IA en termes d'investissement, d'innovation et de main-d'œuvre. À l'heure où les gouvernements des pays membres de l'Alliance relèvent les défis de l'IA, leurs forces armées doivent en faire de même. Au lieu de se contenter de scruter l'horizon, elles doivent investir dans

des initiatives concrètes de recherche, d’expérimentations, de développement et d’adoption de l’IA. Il convient de souligner que tous les efforts en matière d'IA à double usage et d'IA militaire devraient toutefois aborder le plus tôt possible toutes les questions éthiques, juridiques et sociales, y compris les considérations relatives à la vie privée et la définition du niveau de contrôle humain approprié pour toute décision impliquant un recours à la force. Les Alliés devraient envisager d'examiner si un code de conduite éthique pourrait asseoir l'adoption de l'IA dans les forces armées sur des bases plus stables. Au niveau stratégique, les Alliés doivent aussi relever les défis géopolitiques, notamment ceux liés aux investissements de la Chine et de la Russie dans des systèmes militaires faisant appel à l’IA. Comme ce document l'a indiqué, la Russie et la Chine considèrent l'IA comme essentielle pour le futur de leur puissance militaire et investissent massivement dans des systèmes militaires à intelligence artificielle. Pour sa part, la commission des sciences et des technologies de l’AP-OTAN continuera de suivre l'évolution de l'IA dans le secteur de la défense au moyen de visites exploratoires et de témoignages d'experts.

BIBLIOGRAPHIE CHOISIE

Allen, Greg and Chan, Taniel, *Artificial Intelligence and National Security*, Belfer Center for Science and International Affairs, 2017

Allen, Gregory C., *Understanding China's AI Strategy, Center for a New American Security*, 2019

Anderson, Wendy R. and Townsend, Jim, "As AI Begins to Reshape Defense, Here's How Europe Can Keep Up", *Defense One*, 18 mai 2018

Bendett, Samuel, "Putin Drops Hints about Upcoming National AI Strategy", *Defense One*, 30 May 2019

Bendett, Samuel, "The Development of Artificial Intelligence in Russia" in *AI, China, Russia and the Global Order: Technological, Political, Global and Creative Perspectives* (ed.: Wright, Nicholas D.), US DOD and Joint Chiefs of Staff, 2018

Blunt, Richard, Riley, Chris and Richter, Marc, "Using Data Analytics and Machine Learning to Assess NATO's Information Environment", in *Proceedings of the NATO Big Data and Artificial Intelligence for Military Decision Making Specialists' Meeting*, NATO Science and Technology Organisation, 2018

bne IntelliNews, "Russia Raises $2Bln for Investment in Artificial Intelligence", *The Moscow Times*, 31 May 2019

Busby, Mattha and Cuthbertson, Anthony, "'Killer Robots' Ban Blocked by US and Russia at UN Meeting", The Independent, 3 September 2018,

Chen, Nicholas et al., *Global Economic Impacts Associated with Artificial Intelligence*, AnalysisGroup, 2016

CRS (service de recherche du Congrès américain), "U.S. Ground Forces Robotics and Autonomous Systems (RAS) and Artificial Intelligence (AI): Considerations for Congress", CRS, 2018

Cummings, Mary et al., *Artificial Intelligence and International Affairs: Disruption Anticipated*, Chatham House, 2018

Cummings, Mary L., "Artificial Intelligence and the Future of Warfare", in *Artificial Intelligence and International Affairs: Disruption Anticipated* (eds.: Cummings, Mary L. et al.), Chatham House, 2018

De Spiegeleire S., Maas M. and Sweijs T., *Artificial Intelligence and the Future of Defense: Strategic Implications for Small- and Medium-Sized Force Providers*, The Hague Centre for Strategic Studies, 2017

Demchak, Chris C., "Four Horsemen of AI Conflict: Scale, Speed, Foreknowledge, and Strategic Coherence" in *AI, China, Russia and the Global Order: Technological, Political, Global and Creative Perspectives* (ed.: Wright, Nicholas D.), US DOD and Joint Chiefs of Staff, 2018

CESP (Centre européen de stratégie politique), *The Age of Artificial Intelligence: Towards a European Strategy for Human-Centric Machines*, 2018

Franke, Ulrike, *Harnessing Artificial Intelligence*, European Council on Foreign Relations, juin 2019

Govini, *Department of Defense Artificial Intelligence, Big Data, and Cloud Taxonomy*, Govini, 2017

Hoadley, Daniel S. and Lucas Nathan J., *Artificial Intelligence and National Security*, CRS, 2018

Horowitz, Michael C. et al., *Strategic Competition in an Era of Artificial Intelligence*, Center for a New American Security, 2018

IISS, "Big data, artificial intelligence and defence" in *The Military Balance* 2018, IISS, 2018

Insinna, Valerie, "Introducing Skyborg, your New AI Wingman", C4ISRNET, 14 March 2019

Killion, Thomas H., *How AI, Machine Learning and Big Data is Transforming ISR & C2 Capabilities*, ICPQ, 2018

Madni, Azad M., and Madni, Carla C., "Architectural Framework for Exploring Adaptive Human-Machine Teaming Options in Simulated Dynamic Environments", *Systems*, vol. 6, no. 44, 2018

Mercier, Denis, *"How Will Artificial Intelligence and Disruptive Technologies Transform Military Operations and Organizations?"*, in *Proceedings of the NATO Big Data and Artificial Intelligence for Military Decision Making Specialists' Meeting*, NATO Science and Technology Organisation, 2018

Meserole, Chris, *Artificial Intelligence and the Security Dilemma,* Brookings, 2018

Ministère de la défense du Royaume-Uni, *Joint Concept Note 1/18: Human-Machine Teaming*, Development, centre du développement, des concepts et de la doctrine, 2018

Noël, Jean-Christophe, *Intelligence Artificielle : Vers une Nouvelle Révolution Militaire ?*, IFRI, 2018
OMPI (Organisation mondiale de la propriété intellectuelle), Tendances technologiques 2019 – Intelligence artificielle, 2019
Osoba, Osonde A. and Welser IV, William, *Risks of Artificial Intelligence*, RAND, 2017
Payne, Kenneth, *Artificial Intelligence: A Revolution in Strategic Affairs*, *Survival: Global Politics and Strategy*, vol. 60, no. 5, 2018
Pagot, Yves, « Le SCAF raconté par ses concepteurs », Portail Aviation, 31 janvier 2019, http://www.portail-aviation.com/blog/2019/01/31/le-scaf-par-ses-concepteurs/
Renda, Andrea, *Artificial Intelligence: Ethics, Governance and Policy Challenges*, Centre for European Policy Studies, 2019
Sheppard, Lindsey R. et al., *Artificial Intelligence and National Security: the Importance of the Ecosystem*, CSIS, November 2018
Street, Michael et al., "Lessons Learned from Initial Exploitation of Big Data and AI to Support NATO Decision Making" in *Proceedings of the NATO Big Data and Artificial Intelligence for Military Decision Making Specialists' Meeting*, NATO Science and Technology Organisation, 2018
Svenmarck, Peter et al., "Possibilities and Challenges for Artificial Intelligence in Military Applications", in *Proceedings of the NATO Big Data and Artificial Intelligence for Military Decision Making Specialists' Meeting*, NATO Science and Technology Organisation, 2018
Van den Bosch, Karel and Bronkhorst, Adelbert, "Human-AI Cooperation to Benefit Military Decision-Making", in *Proceedings of the NATO Big Data and Artificial Intelligence for Military Decision Making Specialists' Meeting*, NATO Science and Technology Organisation, 2018
Villani, Cédric, *Donner un Sens à l'Intelligence Artificielle : pour une Stratégie Nationale et Européenne*, Mission confiée par le premier ministre Édouard Philippe, La Documentation française, 2018
Welsh, Sean, "Kill Switch", *Jane's Intelligence Review*, March 2018
White, Andrew, "Reality Check: Applying AR and AI technology across the battlespace", *Jane's International Defence Review*, January 2019
Wilson, H. James, Daugherty, Paul R., and Davenport, Chase, "The Future of AI Will Be About Less Data, Not More", *Harvard Business Review*, 14 January 2019