



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

Projet de rapport

**Matej TONIN** (Slovénie)  
Rapporteur

088 STCTTS 19 F | original : anglais | 5 avril 2019

*Tant que ce document n'a pas été adopté par la commission des sciences et des technologies, il ne représente que le point de vue du rapporteur.*

## TABLE DES MATIÈRES

I.	INTRODUCTION .....	1
II.	BREF APERÇU DE L'INTELLIGENCE ARTIFICIELLE .....	2
III.	L'INTELLIGENCE ARTIFICIELLE DANS LES FORCES ARMÉES : OPPORTUNITÉS, DÉFIS ET INCERTITUDES.....	3
A.	LE SOUTIEN EN MATIÈRE D'INFORMATION ET DE DÉCISION .....	3
B.	LES SYSTÈMES AUTONOMES ROBOTISÉS .....	4
C.	LES DÉFIS NON TECHNIQUES DE L'APPLICATION DE L'IA POUR LES FORCES ARMÉES .....	5
D.	LES DÉFIS TECHNIQUES DE L'APPLICATION DE L'IA AUX FORCES ARMÉES .....	6
1.	La vulnérabilité de l'alimentation en données.....	6
2.	Les problèmes de fiabilité .....	7
E.	L'IMPACT POTENTIEL DE L'IA AU NIVEAU STRATÉGIQUE .....	7
IV.	L'IA DANS LES FORCES ARMÉES : APERÇU MONDIAL.....	8
A.	LES ÉTATS-UNIS.....	8
B.	L'EUROPE.....	9
C.	LA CHINE .....	11
D.	LA RUSSIE .....	11
E.	L'OTAN.....	12
V.	REMARQUES FINALES .....	13
	BIBLIOGRAPHIE CHOISIE.....	14

## 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 épisodes de stagnation. Au XXI<sup>e</sup> siècle, en revanche, la recherche, le développement et l'adoption de l'IA ont enregistré une hausse remarquable et prolongée. La recherche a en effet 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 un peu 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 ont été déposées auprès des offices de brevets entre 2013 et 2018 (WIPO, 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 (EPSC, 2018).
- Entre 2016 et 2026, l'impact économique global de l'IA pourrait se situer entre 1,5 milliard 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 » (EPSC, 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, secteur bancaire, divertissements, industrie et fabrication, agriculture, et enfin, réseaux sociaux et numériques (WIPO, 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), et qu'elle pourrait même conduire à redéfinir 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 » (Cummins 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 projet de rapport alimente et complète les travaux menés depuis un certain temps par la STC sur :

- a) les technologies pouvant être sources de rupture qui ont un impact important dans le domaine de la sécurité et la défense ; et
- b) la nécessité pour l'Alliance de conserver son avance scientifique et technologique (voir l'encadré 1).

### Encadré 1 : Travaux connexes de la STC

#### Études 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](#)

#### Études et rapports 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](#)

Ce projet de rapport sera examiné par la commission lors de sa réunion à la session de printemps de l'AP-OTAN en 2019. Une version révisée sera présentée par le rapporteur à l'automne, en vue de son adoption lors de la session annuelle.

## II. BREF APERÇU DE L'INTELLIGENCE ARTIFICIELLE

5. Il n'existe pas de définition communément admise de l'intelligence artificielle. Pour l'essentiel, l'IA 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 » (Cummins, 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 relèvent de différents domaines tels que le traitement du langage humain, la représentation des connaissances, le raisonnement automatique, la vision artificielle et la robotique (Russell et Norvig, 2018). Cela dit, le domaine dans lequel l'IA connaît depuis peu une forte expansion est l'apprentissage automatique, qui recueille 60 % des investissements dans cette technologie (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 l'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. Des exemples courants de ce type d'algorithme sont les systèmes qui, dans les applications d'achat ou de diffusion en continu, 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 Sweijts, 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 (Chatham House, 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 sur les règles (voir l'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 dans les armées du monde entier. Toutes les forces armées modernes s'intéressent pour le moins à l'impact de l'IA, et un grand nombre d'entre elles se dotent de solutions intégrant cette technologie (voir aussi la section IV). L'IA présente un potentiel énorme pour le secteur de la défense, mais aussi tout un éventail de défis (techniques et autres). De surcroît, ses implications sur le plan stratégique sont encore difficiles à cerner.

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

#### Encadré 3 : Comportements du cerveau humain en matière de traitement de l'information (Chatham House, 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.

#### A. LE SOUTIEN EN MATIÈRE D'INFORMATION ET 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 responsables des décisions militaires et stratégiques. Ces systèmes peuvent accroître sensiblement la vitesse et la qualité du traitement, de l'exploitation et de la 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, ce qui peut 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
- Mettre en évidence les tentatives de manipulation des citoyens menées via des campagnes de désinformation.

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 d'une grande fiabilité 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 fonctionnaire 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 de l'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, sont en train de faire évoluer le domaine militaire et stratégique. Cela n'est pas surprenant vu 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/d'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. Plus que toute autre question morale, juridique ou éthique soulevée par l'IA, l'inquiétude suscitée par les systèmes d'armes autonomes létaux (c'est-à-dire des systèmes ayant la capacité de tuer sans qu'il y ait de véritable supervision humaine - voir l'encadré 4) a capté une grande partie de l'attention. Ces armes n'existent pas encore, et aucun État ne veut en concevoir. De plus, un consensus existe au sein de la communauté internationale sur le fait que l'être humain doit conserver un « contrôle digne de ce nom » sur tous les systèmes autonomes, bien que la teneur exacte de ce contrôle reste sujette à débat (Welsh, 2018). Cela dit, un certain nombre de groupes de la société civile et d'États ont préconisé une interdiction préventive de ces systèmes. Ils estiment 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.

19. 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.

20. En novembre 2017, un groupe d'experts gouvernementaux des Nations unies a examiné la question des systèmes d'armes autonomes létaux. À ce jour, une trentaine de pays ont exprimé leur soutien à une interdiction préventive (Busby et Cuthbertson, 2018). 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 discussions au sein du groupe de l'ONU sont au point mort.

#### Encadré 4 : 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.

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

21. 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 rapports, visites et autres activités. Le présent projet de rapport se concentre sur trois de ces défis.

22. **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 % 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).

23. **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 d'entreprises de petite taille et à but commercial. Bien que cette question dépasse le champ d'étude du présent projet de 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 domaines de niche présentant de l'importance sur le plan militaire.

24. **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 de la main-d'œuvre.

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

25. 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

26. 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).

27. Dans la mesure où il est particulièrement difficile de recueillir des ensembles de données qui soient suffisamment volumineux et représentatifs des 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).

28. Même bien entraînés, les algorithmes peuvent être très instables. Un aspect très important – peut-être plus que les autres – 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). À titre d'exemple, un algorithme entraîné exclusivement à l'aide de sources formelles n'est pas capable de comprendre des contenus informels tirés des réseaux sociaux (Hoadley et Lucas, 2018). Pour citer un autre exemple, un système intégrant l'IA a correctement conclu, avec 57,7 % de confiance, qu'une image de panda représentait effectivement un panda. Lorsque l'image a été modifiée de seulement 0,04 % sur sa qualité en pixels, le système



a soudain été convaincu à 99,3 % que l'image représentait un gibbon. On constate donc qu'une modification minime peut induire le système en erreur totale (Noël, 2018).

29. La vulnérabilité de l'alimentation en données est sensiblement exacerbée dans le secteur de la défense. Les données y sont souvent très rares, en comparaison avec le secteur civil. Ainsi, les données dont disposent les forces aériennes sur le comportement de leur aéronef pendant des 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).

## 2. Les problèmes de fiabilité

30. 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. En règle générale, le niveau de confiance doit être beaucoup plus élevé dans le secteur de la défense que dans le domaine civil. Lorsqu'un site de vente en ligne recommande des produits qui n'intéressent pas le consommateur, il n'y a pas grand mal. En revanche, lorsqu'un système militaire intégrant l'IA fait des erreurs, les conséquences peuvent être beaucoup plus graves, et peuvent même aller jusqu'à la perte de vies humaines.

31. 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 fautive 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.

32. 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, la modification même minime 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). 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 peuvent essayer de voler ou de dupliquer leur contenu, que ce soit pour l'intégrer dans leurs propres systèmes ou pour trouver des moyens de neutraliser ces systèmes (Hoadley et Lucas, 2018).

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

33. 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.

34. 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. 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 l'IA imprègne peu à peu le secteur de la défense, les populations pourraient progressivement être moins exposées aux conséquences d'un conflit. Cela pourrait aussi abaisser le seuil de déclenchement de la guerre (Payne, 2018). Troisièmement, l'émergence et l'adoption de nouvelles technologies militaires ont toujours, 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 les 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.

35. 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'acquiescer 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 pas 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.

36. 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**

37. Pour illustrer l'intérêt croissant que suscite l'IA dans les forces armées du monde entier, cette section fournit un bref aperçu des principaux leaders 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**

38. 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.

39. Le département de la défense 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, la DARPA (agence pour les projets de recherche avancée de défense) a annoncé une enveloppe supplémentaire de 2 milliards de dollars pour la période 2018-2023. En 2016, le département 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 ministère en matière d'IA.

40. 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'*US Air Force* 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 pendant une période donnée (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 l'AP-OTAN 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'*US Air Force* a mis sur pied le programme **Skyborg** dont le but est de former les pilotes des avions à l'aide d'un système à base d'IA, qui peut en outre être installé dans un avion 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

41. 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.

42. 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 chefs de file en Europe.

43. 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 de l'éventail 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 d'information 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 très conviviales.
- 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.

44. 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, consacra 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.

45. 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 cyberspace. Il est clair que l'IA jouera également un rôle dans ces travaux.

### C. LA CHINE

46. L'IA est devenue une priorité de premier plan pour les dirigeants chinois. Comme le prévoit le plan de 2017 sur le développement de l'IA de nouvelle génération, la Chine projette de devenir le leader mondial de cette technologie et de développer un marché intérieur de l'IA d'une valeur de 150 milliards de dollars d'ici 2030. Les entreprises installées dans le pays jouent déjà un rôle important dans le développement global de l'IA. La Chine investit non seulement chez elle, mais aussi à l'étranger, ce qui suscite une attention accrue de la part des Alliés.

47. Les liens étroits entre le secteur privé et les institutions publiques (comme l'État-parti et les forces armées) facilitent considérablement l'intégration de l'IA dans le secteur de la défense, car les priorités de développement des entreprises sont clairement définies par un processus de coordination descendant. Cette tendance devrait être accentuée par la volonté du président Xi Jinping de mettre l'accent sur la « fusion civilo-militaire » (Sheppard et al., 2018).

48. Selon les analystes, les efforts accomplis par la Chine pour intégrer l'IA dans son paysage militaire sont largement motivés par la perception qu'ont les Chinois de la stratégie des Américains en la matière. Par conséquent, à l'instar des États-Unis, Pékin s'est focalisé sur le potentiel de l'IA pour améliorer les décisions sur le champ de bataille. Le secteur de la défense chinois travaille en outre beaucoup sur le développement de véhicules autonomes utilisables dans tous les domaines militaires. En 2017, par exemple, une université chinoise ayant des liens avec l'armée a présenté pas moins de 1 000 véhicules aériens sans pilote intégrant l'IA. Il semblerait également que la Chine ait travaillé sur des applications militaires de l'IA dans deux autres domaines : la cybersécurité et les missiles de croisière (Sheppard et al., 2018).

### D. LA RUSSIE

49. Le président Vladimir Poutine a déclaré : « L'IA est l'avenir [...]. Quiconque occupera la première place dans ce domaine deviendra le maître du monde ». Bien que la Russie se situe toujours en retard 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 (moins de 11 millions de dollars à la date de rédaction de ce projet de rapport) (Horowitz et al., 2018).

50. 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 à la date de 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).

51. 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 commandé par intelligence artificielle, capable d'identifier et d'engager des cibles de façon autonome (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

52. 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 contrôle humain significatif, la cyberdéfense faisant appel à l'IA, 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.

53. 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

54. En tant que rapporteure spéciale de la STC, Leona Alleslev avait indiqué au printemps 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.

55. Premièrement, les pays de l'Alliance les plus innovants dans le domaine de la défense doivent conserver leurs positions de leaders. L'Alliance doit disposer des capacités de défense les plus sophistiquées afin d'avoir un pouvoir de dissuasion et, en cas d'échec, de 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 de l'Alliance. Il est encourageant de voir que tous ces pays investissent en fait des ressources substantielles dans ce domaine de la R&D, à l'exception peut-être de l'Allemagne.

56. Deuxièmement, l'écart technologique qui existe entre les Alliés dans le secteur de la défense doit demeurer suffisamment faible pour pouvoir être comblé par l'interopérabilité. La grande diversité des Alliés est en fin de compte l'un des principaux atouts qui font la force de l'OTAN, mais elle signifie aussi qu'il existe de grandes disparités entre les capacités de défense. Le risque est que les investissements massifs effectués dans l'IA par les pays de l'Alliance les plus avancés n'entraînent à l'avenir d'importants problèmes d'interopérabilité. Cela dit, le point positif est que les initiatives en matière d'IA ne nécessitent pas obligatoirement beaucoup d'argent. 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 être en fait une contribution très efficace au partage des charges au sein de l'Alliance. Le rapporteur apprécierait de recevoir des informations sur les initiatives prises en matière d'IA dans le secteur de la défense de la part des délégations concernées.

57. Le secteur de la défense des pays de l'Alliance ne pourra à lui seul relever les défis posés par l'IA qui sont décrits dans ce projet de 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, de développement et d'adoption de l'IA. Au niveau stratégique, les Alliés doivent aussi relever les défis géopolitiques, notamment ceux liés aux investissements de la Chine et de la Russie dans les systèmes militaires faisant appel à l'IA.

## BIBLIOGRAPHIE CHOISIE

(Pour des informations plus exhaustives sur les ressources utilisées, veuillez-vous adresser au personnel du secrétariat international)

- Allen, Greg and Chan, Taniel, [Artificial Intelligence and National Security](#), Belfer Center for Science and International Affairs, 2017
- Anderson, Wendy R. and Townsend, Jim, [“As AI Begins to Reshape Defense, Here’s How Europe Can Keep Up”](#), *Defense One*, 18 May 2018
- 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
- 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](#), Analysis Group, 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 Sweijts 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
- EPSC (European Political Strategy Centre), [The Age of Artificial Intelligence: Towards a European Strategy for Human-Centric Machines](#), EPSC, 2018
- 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
- Jans, Karlijn, [NATO Needs to Get Smarter about AI](#), The Atlantic Council, 2018,
- Killion, Thomas H., [How AI, Machine Learning and Big Data is Transforming ISR & C2 Capabilities](#), ICPQ, 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
- Noël, Jean-Christophe, [Intelligence Artificielle : Vers une Nouvelle Révolution Militaire ?](#), IFRI, 2018
- 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
- Renda, Andrea, [Artificial Intelligence: Ethics, Governance and Policy Challenges](#), Centre for European Policy Studies, 2019
- Russell, Stuart and Norvig, Peter, *Artificial Intelligence: A Modern Approach, Global Edition*, Harlow: Pearson Education Limited, 2018



- 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, 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
- WIPO (World Intellectual Property Organization), [WIPO Technology Trends 2019: Artificial Intelligence](#), WIPO, 2019
-