



Direction du Renseignement
et de la Sécurité de la Défense

ÉPREUVES DE SÉLECTION DES INSPECTEURS DE SÉCURITÉ DE LA DÉFENSE

ANNÉE 2024

Épreuve écrite d'admissibilité : synthèse de dossier et question à réponse courte

Durée 4 heures – coefficient 4

Extrait de l'arrêté du 12 janvier 2021 relatif aux modalités de sélection et de formation des inspecteurs de sécurité de la défense :

« L'épreuve d'admissibilité consiste en une synthèse de dossier composé d'un nombre restreint de documents courts, de types et potentiellement de formats différents (documents rédigés, photos, cartes...), complétée d'une courte rédaction répondant à une question en rapport avec le thème du dossier. Il est tenu compte de l'orthographe, de la compréhension du sujet, de la cohérence des arguments et de la clarté de l'exposé (durée : 4 heures – coefficient 4, note éliminatoire 06/20). Tout candidat ayant reçu une note éliminatoire à cette épreuve ne peut se présenter aux épreuves suivantes et est déclaré ajourné d'office par le collège de sélection au titre de la session de sélection en cours. »

Nota bene : avant de commencer la lecture du dossier, il vous est recommandé d'en vérifier la composition et, le cas échéant, de signaler aux surveillants toute anomalie (page manquante, lecture illisible...).

Il est rappelé que l'anonymat des copies doit être conservé ; il est ainsi interdit de signer sa composition ou d'y mettre tout signe distinctif pouvant donner une indication sur l'identité des candidats.

Les feuilles de brouillon insérées dans les copies ne seront pas corrigées.

L'intelligence artificielle de Défense :
Objectifs, enjeux et limites

Septembre 2024

1. **Synthèse de dossier** (14 points/20)

À partir du dossier joint, dans une note de 800 mots environ ($\pm 10\%$: 720 – 880 mots), vous déclinerez les enjeux de l'intelligence artificielle adaptée au secteur de la défense et vous montrerez quelles en sont les limites et garde-fous nécessaires.

2. **Question à réponse courte** (6 points/20)

Vous répondrez en 200 mots environ ($\pm 10\%$: 180 – 220 mots) à la question suivante :

« Face au déploiement de l'intelligence artificielle, quelles sont les voies suivies par le Ministère des armées pour s'adapter aux nouveaux défis que représentent ces nouvelles technologies ? »

**LE NOMBRE DE MOTS UTILISÉS DEVRA FIGURER SUR LA COPIE,
QUI SERA IMPÉRATIVEMENT REDIGÉE À L'ENCRE NOIRE**

DOSSIER DOCUMENTAIRE

8 documents – 25 pages

(pages 4 à 28)

Document 1	Défense : les start-up de l'intelligence artificielle tentent d'investir le champ de bataille Le Monde – juin 2023	Pages 4 à 7
Document 2	« L'intelligence artificielle transforme les paradigmes traditionnels de la guerre » Le Monde – janvier 2024	Pages 8 à 10
Document 3	Blindés connectés, «débruitage» des communications... Thales accélère dans l'IA de défense et crée CortAix Le Figaro – mars 2024	Pages 11 à 13
Document 4	IA : « Soit l'armée française prend date, soit elle décroche », affirme Sébastien Lecornu Les Echos – mars 2024	Pages 14 à 16
Document 5	Intelligence artificielle: les eurodéputés adoptent une loi "pionnière" Le Nouvel Obs – mars 2024	Pages 17 à 18
Document 6	Risquées, les armes contrôlées par l'IA? Ce qu'il faut savoir Science Presse – novembre 2023	Pages 19 à 22
Document 7	L'intelligence artificielle et le monde de la défense www.entreprises.gouv.fr – juin 2023	Pages 23 à 24
Document 8	L'ONU veut réguler l'intelligence artificielle militaire mais se heurte au principe de réalité concurrentielle Revue Conflits – Août 2023	Pages 25 à 28

Défense : les start-up de l'intelligence artificielle tentent d'investir le champ de bataille

Des entreprises proposent d'ajouter des logiciels d'IA sur des équipements déjà opérationnels, afin de gagner en efficacité et de mobiliser moins de ressources.

Par Elise Vincent et Jean-Michel Bezat

Le Monde - 27 juin 2023

Antoine Bordes aurait pu continuer à se partager entre Paris et New York, où cet expert renommé de l'intelligence artificielle (IA) dirigeait le laboratoire Facebook Artificial Intelligence Research du groupe Meta. Et puis, l'invasion de l'Ukraine par la Russie a eu un profond écho en lui et l'a poussé à retraverser l'Atlantique. Les valeurs démocratiques en danger, la souveraineté technologique de l'Europe face aux hyperpuissances américaine et chinoise... Tous ces périls l'interpellaient. « *Si ce que je sais faire peut avoir un impact sur la défense française et européenne, je suis dix fois plus motivé* », explique-t-il, trois mois après sa nomination comme vice-président de Helsing pour la recherche.

Cette start-up est encore sous les radars. Née à Berlin, en 2021, grâce à un investissement de 100 millions d'euros du fonds Prima Materia du fondateur de Spotify, le Suédois Daniel Ek, elle s'est implantée au Royaume-Uni et en France.

Ce triple ancrage permet à cette entreprise de travailler dans les trois pays alignant les forces militaires les plus importantes du Vieux Continent. Avec ses 220 salariés, dont 150 ingénieurs, et des recrutements de haut niveau, comme celui de l'ancien chef d'état-major de l'armée de l'air française, le général Denis Mercier, Helsing veut permettre aux armées de « *réaliser des gains capacitaires importants* » grâce aux ressources encore inexploitées de l'IA sur le champ de bataille.

La société vient d'être sélectionnée par le ministère de la défense allemand. En partenariat avec Saab Germany, qui fournit les capteurs, son logiciel d'IA va renforcer les radars de quinze Eurofighter de la Luftwaffe destinés à remplacer les Tornado pour les missions de neutralisation des défenses aériennes adverses. A partir de 2028, le système embarqué sur ces avions de chasse (et non dans le cloud) sera capable d'analyser les données radars recueillies « *pour générer, en quelques millisecondes, des mesures d'autoprotection précises contre les radars ennemis modernes* », expliquent ses concepteurs.

« Amplifier l'efficacité des matériels existants »

Une telle « couche logicielle » permettrait aussi d'améliorer l'efficacité des chaînes d'artillerie, constituées notamment des canons Caesar (155 mm), par l'accélération de la boucle renseignement-feu. Elle entraînerait une réduction des stocks de munitions

nécessaires et offrirait une meilleure protection contre les tirs de contrebatteries, selon Helsing. En mer, cela améliorerait la protection des frégates contre les redoutables essaims de drones armés.

La multiplication des capteurs, sonars et radars met de plus en plus les militaires devant un « mur de données ». Ils doivent les traiter dans l'urgence des combats, où la rapidité de décision est déterminante.

L'objectif est d'ajouter ces logiciels d'IA sur des équipements déjà opérationnels. *« L'IA permet d'amplifier de manière significative l'efficacité des matériels existants, sans attendre les capacités futures »*, souligne Antoine de Braquilanges, directeur général de Helsing France. *« L'adaptation peut intervenir très rapidement, nous ne sommes pas dans une vision à 2040 »*, confirme son président, Marc Fontaine, ancien responsable de la transformation numérique d'Airbus. Et elle mobilise bien moins de ressources que les grands programmes s'étalant sur des décennies et engageant des dizaines de milliards d'euros. *« Dans le cas de l'IA embarquée, on parle de dizaines de millions d'euros, tout au plus de centaines de millions »*, plaide-t-il.

Malgré la hausse des crédits de la loi de programmation militaire (LPM) 2024-2030 (413 milliards d'euros courants), les contraintes budgétaires empêchent de répondre à tous les besoins capacitaires des armées, qui resteront « échantillonnaires ». Ce qui justifie une utilisation optimale des matériels. Une couche d'IA supplémentaire pourrait être intégrée dans le cadre de la rénovation des équipements (chars Leclerc...) ou du programme Scorpion de livraison à l'armée de terre des nouveaux véhicules blindés (Serval, Griffon, Jaguar).

« Ce n'est qu'un ingrédient dans une recette »

La start-up demande à pouvoir faire ses preuves en condition opérationnelle, explique Marc Fontaine : *« Fixer un cadre d'expérimentation, mettre en commun les compétences métiers des armées et l'IA, valoriser des cas d'usage et aller voir la direction générale de l'armement [DGA] et les armées pour passer au stade industriel. »*

Plus largement, Helsing souhaite mieux *« intégrer l'intelligence artificielle dans la base industrielle et technologique de défense »*. Et notamment collaborer avec ses poids lourds (Dassault Aviation, MBDA, Nexter, Naval Group, Airbus, Thales...), qui portent les « programmes à effets majeurs » (Rafale ou A400M, frégates, sous-marins nucléaires, véhicules blindés, systèmes antimissiles...).

De grandes entreprises de la défense se montrent à la fois intéressées et prudentes face à des sociétés très agiles ne travaillant pas dans les mêmes temporalités. *« Il y a beaucoup de communication de la part de Helsing, dit le PDG d'un groupe d'armement. Ce logiciel, ce n'est qu'un ingrédient dans une recette. »* Il doit s'intégrer à un avion, à un navire ou à un blindé.

Un argument revient : on n'a pas attendu pour développer l'IA. Mais les jeunes pousses de la « deftech » invitent les grands groupes à méditer les leçons de ChatGPT : 300

talents d'OpenAI ont devancé des milliers d'ingénieurs de Google, de Meta et de Microsoft dans l'IA générative, obligeant ces géants à accélérer la mise au point de nouveaux outils ou à s'associer aux start-up. *« L'une des principales leçons de l'accord avec Saab, répond Marc Fontaine, c'est qu'une petite société de la "deftech" a pu être partenaire d'un industriel de premier plan, qui a vu nos complémentarités et testé notre système. »*

Au ministère des armées, on fait remarquer que l'IA est déjà largement intégrée. Si elle n'a pas de ligne budgétaire spécifique dans la LPM, l'innovation y est présentée comme prioritaire, avec 10 milliards d'euros sur six ans. *« Elle s'appuiera sur le développement de démonstrateurs ambitieux et l'accélération du déploiement de ces innovations dans les armées »,* explique l'annexe à la loi. Responsable de la cellule de coordination de l'IA au sein de l'Agence de l'innovation de défense, Michaël Krajecki souligne que *« ce n'est plus identifié comme un objet particulier »* et que *« cela fait toujours partie des briques que l'on développe »*.

Stratégie nationale

Une stratégie nationale a été définie, en 2018, avec des domaines prioritaires, explique-t-il : la santé des soldats, qui intègre surtout le suivi des unités opérationnelles ; le combat collaboratif, avec l'environnement Scorpion et la veille collaborative navale *« où des travaux sont en cours »* ; la logistique, le soutien et le maintien en conditions opérationnelles, où d'importants efforts ont été faits pour accroître la disponibilité de matériels (hélicoptères...) ; le cyber et l'influence dans le cadre de la lutte informationnelle ; la robotique ; et l'activité cruciale du renseignement.

Sur ce point, une start-up française est bien positionnée : Preligens. Créée en 2016 sous le nom d'Earthcube, elle est spécialisée dans le traitement de différents types de données (ondes électromagnétiques, images provenant de capteurs infrarouges, de radars, de drones et de satellites, textes tirés de la veille sur Internet...). Le fonds d'investissement du ministère, Definvest, avait participé au financement de cette société présentée par Florence Parly, alors ministre des armées, comme une *« pépite nationale »* stratégique.

Preligens a signé, en octobre 2022, un contrat de 240 millions d'euros avec la DGA pour mettre ses savoir-faire au service du renseignement géospatial (par satellite) des armées. Après plusieurs années de développement laborieux, cette brique doit être intégrée au projet Artemis.IA, qui va doter les armées, notamment le renseignement militaire, d'une solution souveraine et sécurisée de traitement massif de données.

Les experts affirment que l'IA va *« changer la donne »* en modifiant l'équilibre des forces, sur le champ de bataille et au-delà. Certains la jugent même aussi disruptive que la poudre noire inventée par les Chinois (et, donc, les armes à feu) ou l'arme nucléaire. C'est l'analyse que faisait Eric Schmidt, ancien PDG de Google, qui a été le premier président du Defense Innovation Board, créé en 2016 pour infuser l'esprit d'innovation au sein du Pentagone.

Les « leçons de la guerre en Ukraine »

« On commence à tirer beaucoup de leçons de la guerre en Ukraine », terrain d'expérimentation sans précédent des technologies numériques, constate Antoine de Braquilanges, cependant très discret sur l'implication de Helsing dans cette guerre.

L'agilité de l'armée ukrainienne et sa capacité à intégrer des innovations au combat, compensant une « masse » inférieure à celle des forces russes, se sont révélées déterminantes. Kiev a créé un portail ouvert aux innovations des civils. Dès le début de la guerre, le pays a déployé l'application GIS Art for Artillery, connectant les observateurs sur le front avec les batteries, améliorant la localisation des cibles, divisant par dix le temps de coordination et démultipliant l'efficacité des frappes.

Depuis un an, les investisseurs rechignent moins à financer les entreprises de défense. Les capitaux affluent dans la « deftech », surtout aux Etats-Unis. Fin 2022, Anduril Industries, l'une des plus actives, a levé 1,5 milliard de dollars (1,38 milliard d'euros). Dans un rapport intitulé « Relancer l'arsenal de la démocratie », slogan assez proche des engagements de Helsing, la société souligne qu'« *il y a plus d'intelligence artificielle dans une Tesla que dans un véhicule de l'US Army* » et plaide pour davantage de logiciels IA embarqués. Elle vient de rapprocher son système de traitement des données Lattice de la plate-forme de renforcement des réseaux télécoms Spacetime d'Aalyria, spin-off de Google, pour sécuriser et accélérer les communications en milieux hostiles.

De son côté, Shield AI va fournir à Boeing Defense, Space & Security son pilote numérique Hivemind, une capacité de mise en réseau entre les systèmes sur un théâtre d'opérations et capable de fonctionner sans données GPS dans des environnements de combat, assure l'entreprise créée en 2015 à San Diego, en Californie. Déjà embarqué sur des F-16 et des drones à décollage vertical, Hivemind équipera les aéronefs de nouvelle génération, avec ou sans pilote. « *Il ne faut pas perdre cinq à dix ans quand une société, focalisée sur un objectif, permet d'aller plus vite et plus loin* », prévient Antoine de Braquilanges.

« *L'Europe – et la France en particulier – n'a rien à envier aux Etats-Unis dans le domaine de l'intelligence artificielle*, assure Antoine Bordes. *J'ai l'ambition de faire émerger un champion européen de l'IA de défense.* » Historiquement, ce sont des innovations militaires qui sont devenues des applications grand public, comme Internet ; désormais, les avancées du secteur civil irrigueront de plus en plus les armées.

« L'intelligence artificielle transforme les paradigmes traditionnels de la guerre »

Tribune

Pour relever les défis posés par l'IA dans le domaine de la guerre et de la sécurité, Eric Autellet, général de l'armée de l'air, et Alexandre Papaemmanuel, enseignant et administrateur de Défense Angels, appellent, dans une tribune au « Monde », à faciliter la collaboration entre les secteurs civil et militaire.

Le Monde - 31 janvier 2024

L'intelligence artificielle (IA) façonne de manière profonde le paysage des conflits modernes, offrant un ensemble de capacités inédites pour renforcer la sécurité. Des drones autonomes aux systèmes de surveillance avancés, l'IA transforme les paradigmes traditionnels de la guerre et soulève des questions cruciales quant à l'avenir des conflits, la place de l'humain dans le processus de prise de décision, et les implications éthiques qui en découlent.

La nature des données militaires – confidentielles par essence et protégées par nécessité – peut être un frein à l'opérationnalisation de l'IA. Secret, sécurité, sensibilité peuvent transformer les armées en forteresse hermétique aux répercussions d'une innovation civile s'imposant sur les théâtres d'opération contemporains.

Aujourd'hui, les opérateurs de drones ukrainiens s'appuient sur les algorithmes pour corriger automatiquement les trajectoires de leurs munitions rôdeuses. Le commandement ukrainien utilise l'IA pour proposer des options opérationnelles. Les soldats tirent parti d'algorithmes embarqués dans des satellites pour détecter les mouvements ennemis. La robotisation du champ de bataille, couplée au déploiement massif de l'IA, ouvre une nouvelle ère où le soldat se voit augmenté. La réalité de cette course aux algorithmes de défense pousse les armées à opérationnaliser rapidement ces technologies pour garantir un avantage significatif.

Talents et supercalculateurs

Comme jadis pour le contrôle de l'atome, la France, consciente de l'importance de l'IA dans le contexte militaire, a inscrit dans la loi de programmation militaire 2024-2030 la nécessité de maîtriser cette technologie, aux côtés des systèmes autonomes et du calcul quantique. Cependant, ces ambitions posent des défis considérables, notamment en matière de ressources humaines qualifiées, de transformation et de relation avec le secteur privé dans un contexte d'économie de défense.

Pour relever ces défis, la France, forte de son excellence académique dans le domaine de l'ingénierie, possède un vivier de compétences mondialement reconnu. Mais mobiliser ces talents au service des armées nécessite une refonte en profondeur des

politiques de recrutement, de formation continue, de management et de carrière au sein des institutions militaires et de l'industrie de défense.

Le ministère des armées travaille déjà au développement d'algorithmes d'IA et a intégré le changement de paradigme induit par l'intelligence artificielle dans les systèmes d'armes. Cette évolution doit se poursuivre en cohérence avec les avancées technologiques du secteur civil. Au-delà de la conquête des talents, il est nécessaire de conquérir des capacités de calcul, des serveurs et des supercalculateurs pour accueillir données, logiciels et algorithmes, éléments indispensables à la mise en œuvre d'une stratégie d'IA conquérante.

Cette montée en puissance des moyens et des ressources du ministère des armées permettra de lever progressivement les barrières entre le secteur civil et militaire. En facilitant la collaboration entre les parties prenantes, en tirant parti des méthodes de traitement massif des données, de l'IA ou du jumeau numérique, les données deviennent un terrain d'innovation croisée prometteur. Il est essentiel d'encourager les acteurs du secteur à concevoir des cadres de confiance adaptés, favorisant l'innovation collaborative par le biais des données.

Ces écosystèmes, qu'ils soient ouverts, semi-ouverts ou fermés, selon les besoins, viseront à générer un impact positif au sein d'une communauté de confiance de l'IA de défense. Ils favoriseront un partage plus efficace entre laboratoires, recherche, start-up, grandes entreprises et administrations.

Equilibre public-privé schizophrénique

Dans le cadre de cette « guerre de l'IA », l'armée américaine a mis en œuvre le plan ambitieux « Replicator », visant à développer une armée de 2 000 chasseurs pilotés par des machines. Ce projet a ouvert la voie à une nouvelle génération d'entreprises collaborant étroitement avec l'armée pour fournir des solutions innovantes mêlant drones, algorithmes, nouveaux matériaux et technologies de propulsion au profit de la Next Generation Air Dominance (« nouvelle génération de domination aérienne », NGAD).

Une dynamique collective d'IA de confiance peut ainsi favoriser l'émergence d'un numérique de combat assumant pleinement son rôle de catalyseur dans l'innovation numérique au profit des armées. Cela nécessite la mise en place d'un échange public-privé équilibré et maîtrisé.

Par son déferlement, l'IA impose un équilibre public-privé schizophrénique imposant le renforcement de l'autonomie des armées comme préalable indispensable à l'accueil des innovations extérieures. Malgré ses remparts, la forteresse doit s'ouvrir pour animer un écosystème complexe mêlant coopération et concurrence. Demain, la ligne de défense se pensera également sans uniforme, en nouant des partenariats avec des administrations partenaires, des alliés internationaux, des industriels établis et des start-up innovantes afin de canaliser le foisonnement de l'IA. Ce bastion pourra être à la convergence de divers milieux, afin de stimuler une culture administrative créatrice tout en renouvelant le tissu économique établi.

En mobilisant l'ensemble des communautés, en concevant des cadres de confiance adaptés, la France pourrait ainsi se positionner dans la course aux algorithmes et garantir sa supériorité opérationnelle dans la guerre d'aujourd'hui et celles de demain. C'est à ces conditions que les militaires, experts, universitaires et ingénieurs pourront se mobiliser pour que, demain, la France et les armées françaises puissent tenir leur rang dans cette course aux algorithmes.

Blindés connectés, « débruitage » des communications... Thales accélère dans l'IA de défense et crée CortAix

Par Véronique Guillermand

Le Figaro 28/03/2024

Le leader européen de l'intelligence artificielle dédiée aux industries critiques accompagne la mutation 4.0 des armées, en s'appuyant sur les compétences de 600 experts.

Orchestrer des milliers de décollages et atterrissages d'avions (40.697 sur le seul mois de juillet 2023 à Roissy Charles de Gaulle) en évitant les «files» d'attente dans le ciel, afin d'optimiser la consommation de carburant et fluidifier le trafic aérien. Planifier une mission de renseignement militaire, en prenant en compte la topographie, la météo, les positions et mouvements amis ou ennemis des différents acteurs du champ de bataille, dans plusieurs dimensions (air, terre, mer, espace et cyber). Classifier et détecter tous les mouvements aériens à plus de 200 km à la ronde, en ne confondant pas la signature électromagnétique d'un drone avec celle d'un oiseau, dans le cadre de la défense anti-aérienne d'une ville. C'est mission impossible pour le cerveau humain, saturé par un déluge de données.

Depuis des décennies, les contrôleurs aériens, les chefs d'état-major des armées, les opérateurs de radars militaires sont assistés par des ordinateurs. Et plus récemment par des algorithmes intelligents, capables d'extraire les données pertinentes et de proposer des plans d'actions. Et, cela, en une poignée de seconde. Ces IA dédiées aux systèmes critiques doivent être fiables et sécurisées mais aussi être capables de justifier, de façon simple, leur préconisation.

C'est le terrain de jeu de Thales, leader européen de «l'IA de confiance», qui embarque des technologies à base d'IA dans une centaine de systèmes et capteurs depuis une dizaine d'années. Le groupe de défense veut accélérer avec des IA de nouvelle génération dédiées aux industries critiques : défense, aéronautique, spatiale, identité numérique. Dans le militaire en particulier, le groupe se place en partenaire de la transformation 4.0 des armées. En octobre 2023, Thales et ses partenaires ont testé, avec succès, un démonstrateur de « *planification dynamique* » d'opérations militaires à base d'IA, pour le compte de l'Otan, dans le cadre de l'exercice Steadfast Jupiter 23

Numérisation des armées

La défense se numérise en effet rapidement. À l'instar de l'armée de Terre qui se modernise, dans le cadre du programme Scorpion. Les nouveaux blindés Jaguar et Griffon, qui entrent en service progressivement, sont des véhicules connectés et cybersécurisés. À horizon 2040, le Système de combat aérien du futur (Scaf) et son

homologue terrestre, le MGCS, opéreront au sein d'un cloud de combat, interconnectant tous les acteurs du champ de bataille.

C'est dans ce cadre, que Thales a annoncé, ce jeudi matin, la création d'une nouvelle entité, baptisée CortAlx, qui rassemble les forces vives du groupe dédiées à l'IA. Il s'agit « d'un accélérateur » dont l'objectif est d'amplifier l'intégration de l'IA dans l'ensemble des systèmes, capteurs et produits développés par les divisions du groupe. « *Nous avons déjà construit une expertise de tout premier plan avec plus de 600 experts en IA et plus de 100 doctorants. Thales est le plus grand acteur européen de l'IA de confiance dédiée aux systèmes critiques et occupe le premier rang en termes de dépôts de brevets, dans ce domaine* », explique Patrice Caine, PDG de Thales, au *Figaro*.

CortAlx est doté de trois bras armés. D'abord, CortAlx Lab, qui intègre « *le plus puissant laboratoire intégré dans le domaine de l'IA critique* », basé sur le plateau de Saclay, à côté de Paris. En plus du pilotage des programmes de R&D, le laboratoire réalise, avec des équipes de hackers « éthiques », des « stress-tests », simulant des cyberattaques, afin de tester la capacité de résistance des IA et détecter d'éventuelles failles. Ils s'entraînent sur les IA conçues par Thales mais aussi celles déployées dans le monde civil. Dernier exploit en date de ces « gentils hackers » : le piratage de ChatGPT, le robot conversationnel, développé par OpenAI.

L'accélérateur s'appuie aussi sur une CortAlx factory, une usine technologique, dont la mission est d'identifier de nouvelles applications. Ses équipes ont gagné, en 2023, un concours organisé par la Direction générale de l'armement (DGA) en développant un système de pilotage à base d'IA de drones aériens et de robots terrestres, agissant en essaim et capables de communiquer entre eux.

Le « carré magique » de l'IA

CortAlx sensors, complète le dispositif. Ce département est en charge des capteurs – sonars, radars et radios – développés par le groupe pour ses clients militaires. Ce département travaille par exemple sur l'intégration de l'IA dans les radios tactiques des forces armées. Objectif « débruiter » les communications, en gommant les bruits parasites. Il a aussi amélioré les capacités du pod Talios, destiné aux missions de reconnaissance aérienne et de ciblage. Ce système, qui équipe l'avion de combat Rafale, collectait jusqu'ici des images analysées au sol. Grâce au « processeur neuronal », développé par Thales, les données sont analysées en temps réel par l'IA embarquée. Et, cela, cent fois plus vite que sa version précédente.

Pour rester aux avant-postes de l'IA des systèmes critiques, Thales dispose d'atouts majeurs, qui forment un « *carré magique* », selon l'expression de Patrice Caine. Le groupe met en avant sa connaissance intime des métiers et des besoins de ses clients ainsi que des environnements contraints dans lesquels ces systèmes et capteurs sont embarqués et utilisés, par exemple à bord d'un sous-marin, d'un drone ou d'un système de guidage de missile.

Il revendique également une expertise technologique de bout en bout. « *Dans les sonars par exemple, la compréhension de la propagation des ondes acoustiques et de la physique des matériaux qui composent les sonars est clef pour développer une IA*

pertinente et adaptée. Il existe en effet un lien entre le monde physique et les algorithmes », développe le PDG. Enfin, Thales s'appuie sur ses compétences en cybersécurité, un domaine où il fait partie du Top-5 mondial, avec 5 800 experts dédiés. « Il n'y a pas d'IA de confiance, sans cybersécurité. Sans compétences cyber, il est impossible de se présenter comme un acteur crédible », insiste Patrice Caine.

L'homme reste décisionnaire

« L'IA se déploie rapidement aujourd'hui dans les systèmes critiques pour deux raisons principales : tous les capteurs sont passés du monde analogique à celui du numérique, qui génère des flux de données massives, et, dans le même temps, les progrès des capacités de calcul des composants permettent de réaliser les traitements directement dans les capteurs, sans avoir à rapatrier ces données dans un data center ou le cloud », développe Patrice Caine. Thales a conçu des technologies basées sur des processeurs neuronaux, l'équivalent d'un composant dont ses équipes ont totalement réécrit et cyberprotégé la couche logicielle. Cela, afin de s'assurer de l'autonomie de décision de l'opérateur humain. « Les IA de systèmes critiques relèvent de la sécurité et de la souveraineté. L'enjeu peut être vital, contrairement aux IA génératives de contenus, d'images et de sons utilisées par le grand public », développe le PDG du groupe, dont les IA, assure-t-il, ne prennent jamais la décision finale. « C'est toujours l'humain, qui est aux commandes, qui valide la décision », conclut-il.

IA : « Soit l'armée française prend date, soit elle décroche », affirme Sébastien Lecornu

Le ministre des Armées, Sébastien Lecornu, annonce dans « Les Echos » la création d'une agence dédiée à l'intelligence artificielle militaire, ainsi que l'achat d'un super ordinateur pour faire de l'IA « classifiée » à partir de données secret-défense.

Par Anne Bauer, Julien Dupont-Calbo

Les Echos - 8 mars 2024

Sur terre, sur mer, dans les airs ou à l'arrière, l'irruption et surtout les perspectives de l'IA devraient bouleverser la manière de faire la guerre. Pour être au rendez-vous, la France muscle son arsenal avec un nouveau plan, que Sébastien Lecornu, le ministre des Armées, dévoile aux « Echos » avant la présentation ce vendredi devant les élèves de Polytechnique qui ont un rôle à jouer là-dedans.

Qu'allez-vous annoncer aux élèves de l'Ecole polytechnique ?

Que la France et ses armées doivent se battre pour garder notre rang. Il nous faut avoir les briques technologiques pour basculer souverainement sur les nouvelles générations d'armement. Les armées doivent prendre le virage de l'intelligence artificielle, c'est pourquoi j'annonce la création d'une nouvelle agence ministérielle pour l'IA de défense, l'Amiad.

Soit on prend date tout de suite, soit on décroche. C'est dans ce cadre qu'un travail inédit est mené depuis 2017 sur l'intelligence artificielle, avec une accélération forte depuis un an et en prenant pour comparaison et modèle ce qui s'est fait avec l'atome dans les années 1960.

Comment fonctionnera cette agence ministérielle ?

La nouvelle agence sera directement sous ma tutelle, comme l'est la Direction des applications militaires (DAM) du CEA. La DAM, qui fabrique des têtes nucléaires, est le dernier arsenal français.

L'Amiad en sera un autre : elle doit conceptualiser, voire fabriquer l'intelligence artificielle dans les grands programmes militaires, actuels comme futurs. D'ici à 2026, elle a vocation à recruter 300 ingénieurs, chercheurs, doctorants civils et militaires. Elle fonctionnera avec une grande souplesse pour convaincre les meilleurs talents de venir y travailler.

Un pôle recherche sera établi à Palaiseau, sur le site de l'Ecole polytechnique, tandis qu'un pôle technique sera situé à Bruz, à côté de Rennes, sur le site spécialisé dans la maîtrise de l'information et la cyber de la Direction générale de l'armement (DGA).

De quels moyens disposera-t-elle ?

L'agence sera dotée de moyens importants, avec une enveloppe d'environ 300 millions d'euros par an. On va consacrer 2 milliards d'euros pour l'intelligence artificielle en matière de défense entre 2024 et 2030. Mais surtout, elle sera dotée de son propre super ordinateur classifié. Situé au Mont-Valérien à Suresnes, il permettra de traiter souverainement des données secret-défense.

Un plan pour l'IA militaire avait déjà été lancé en 2019. Était-il insuffisant ?

Il a permis à de nombreux projets d'émerger au sein des armées. Le ministère des Armées recense déjà plus de 400 cas d'usage, du stade de l'idée au développement en cours.

Mais il s'agit désormais de passer à l'âge adulte et de construire un outil qui sera au service de l'armée française, de la DGA, de la DGSE, de notre industrie de défense, voire des entreprises privées du secteur civil, qui ont besoin d'un espace protégé.

Quels seront les champs d'activité de l'agence ?

L'IA réinterroge tous les équipements de l'armée, du Rafale au sous-marin nucléaire jusqu'au drone miniaturisé des forces spéciales.

Prenez l'exemple des oreilles d'or, ces sous-marinières capables à l'oreille de tracer la signature acoustique d'un sonar de sous-marin d'un autre pays. Nos premiers essais en matière d'IA appliquée à l'acoustique sous-marine sont bouleversants, qu'il s'agisse de vérifier ce qu'un humain a déjà détecté ou de donner un diagnostic bien plus rapidement.

Admettons que l'IA parvienne à de meilleurs diagnostics que l'oreille d'or et que ce soit votre adversaire qui la possède, tous vos investissements dans des sous-marins de troisième génération deviendraient relatifs. Plus l'IA devient puissante, plus elle risque de remettre en cause des équipements qu'on pensait établis.

Elle bouleversera même les états-majors. Lorsqu'on voit le nombre d'officiers d'états-majors qui se penchent autour d'une carte pour la planification d'opérations, on peut penser que l'IA pourrait les aider... Ne serait-ce que dans la rédaction de leurs notes de synthèse, afin de dégager plus de temps pour les fonctions militaires et moins pour les tâches administratives.

Des applications civiles, duales, seront sans doute possibles...

L'intelligence artificielle pourra être mise au service de la gestion de ce ministère de 260.000 personnes. L'IA doit ainsi permettre une meilleure maintenance de nos équipements. Si demain, l'ordinateur interne d'un A400M ou d'un Rafale offre un autodiagnostic, cela permettra d'adapter bien plus intelligemment les révisions et les réparations et d'opérer une révolution dans la gestion des pièces de rechange. Cela intéressera sans doute des compagnies aériennes civiles...

Les leçons tirées de la guerre en Ukraine peuvent-elles inspirer l'agence ?

C'est déjà le cas. Par exemple, sur la guerre des drones. Ceux-ci sont très vite brouillés. Un drone doté d'IA qui serait capable de continuer sa mission une fois qu'il a perdu le contact avec son pilote, serait bien plus redoutable qu'un drone sans IA ! Le canon

Caesar est un autre exemple intéressant. On a des problèmes d'obus en Ukraine. Le meilleur remède serait d'en consommer moins. S'il vous faut 10 obus pour marquer votre cible ou si vous arrivez à le faire dès le premier coup, cela change la donne. Il y a un travail en cours pour que l'intelligence artificielle assiste l'artilleur en facilitant le verrouillage de la cible.

L'IA se développe aujourd'hui dans le secteur privé. Elle n'a pas attendu un grand plan militaire...

C'est exact. Si l'IA a sans doute bénéficié de financements militaires aux Etats-Unis, elle se développe surtout grâce aux Gafam. Mais pensez-vous, par exemple, que l'on puisse confier le développement de l'IA dans le domaine de la dissuasion à des entreprises comme Google ? Non, bien entendu ! Le plan que je veux défendre ne vise pas à concurrencer les initiatives privées. L'enjeu est ni plus ni moins que de garantir la survie du modèle souverain et autonome de la défense française.

Anne Bauer et Julien Dupont-Calbo

Intelligence artificielle: les eurodéputés adoptent une loi "pionnière"

Nouvel Obs et AFP, 13 mars 2024

Les députés européens ont adopté mercredi des règles pour encadrer les systèmes d'intelligence artificielle (IA) comme ChatGPT, une législation unique au monde.

Le commissaire européen chargé du dossier, Thierry Breton, s'est félicité sur X du "soutien massif" du Parlement (523 voix pour, 46 voix contre) au texte.

"Cela profitera au formidable réservoir de talents de l'Europe. Et établira un modèle pour une IA digne de confiance dans le monde entier", a souligné de son côté la présidente de la Commission européenne Ursula von der Leyen, évoquant une législation "pionnière".

Ce projet de loi avait été présenté par la Commission européenne en avril 2021. L'apparition fin 2022 de ChatGPT de la start-up californienne OpenAI, capable de rédiger des dissertations, poèmes ou traductions en quelques secondes, lui a donné une nouvelle dimension.

Ce système a révélé l'énorme potentiel de l'IA mais aussi ses risques. La diffusion de fausses photos ou vidéos, plus vraies que nature, a ainsi alerté sur le danger de manipulation de l'opinion.

"Que le commencement"

Le président français Emmanuel Macron a salué le vote, évoquant "une première au monde, indispensable pour protéger les droits de chacun et la sécurité des données tout en soutenant l'innovation". "C'est l'Europe qui le fait!", a souligné sur X le chef de l'Etat qui avait pourtant, au lendemain de l'accord sur cette législation en décembre, estimé que ce n'était "pas une bonne idée" de vouloir "beaucoup plus réguler que les autres" pays.

Avec ce texte, "nous avons réussi à trouver un équilibre très fin entre l'intérêt d'innover et l'intérêt de protéger", a aussi estimé le co-rapporteur Dragos Tudorache (Renew, centristes et libéraux).

Toutefois, cette législation "n'est que le commencement", a-t-il relevé, rappelant que l'intelligence artificielle continuait d'évoluer rapidement.

Le règlement prévoit une approche à deux niveaux. Les modèles d'IA à "usage général" devront respecter des obligations de transparence ainsi que les règles européennes en matière de droits d'auteur.

Quant aux systèmes considérés à "haut risque" - utilisés par exemple dans les infrastructures critiques, l'éducation, les ressources humaines, le maintien de l'ordre - , ils seront soumis à des exigences plus strictes.

Ils devront par exemple prévoir la mise en place d'une analyse d'impact obligatoire sur les droits fondamentaux.

Les images, textes ou vidéos générés artificiellement ("deep fakes") devront être clairement identifiés comme tels.

Le texte interdit les systèmes de notation citoyenne ou de surveillance de masse utilisés en Chine, ou encore l'identification biométrique à distance des personnes dans les lieux publics.

Sur ce dernier point, les Etats ont toutefois obtenu des exemptions pour certaines missions des forces de l'ordre comme la prévention d'une menace terroriste ou la recherche ciblée de victimes.

La législation européenne sera dotée de moyens de surveillance et de sanctions avec la création d'un office européen de l'IA, au sein de la Commission européenne. Il pourra infliger des amendes allant de 7,5 à 35 millions d'euros, en fonction de l'infraction et de la taille de l'entreprise.

"Nous réglémentons le moins possible, mais autant que nécessaire", a résumé M. Breton.

"Lacunes, restrictions et exceptions"

Le Bureau européen des unions de consommateurs (BEUC) a cependant estimé que "la législation aurait dû aller plus loin pour protéger les consommateurs".

"Le texte final est plein de lacunes, de restrictions et d'exceptions, ce qui signifie qu'il ne protégera pas les personnes, ni leurs droits humains, contre certaines des utilisations les plus dangereuses de l'IA", a estimé en écho le groupe de défense des droits numériques Access Now.

De son côté, Markus J. Beyrer, directeur général de BusinessEurope, la voix du patronat européen, a estimé qu'il s'agissait d'un "moment charnière pour le développement de l'IA en Europe".

L'Observatoire des multinationales (France), Corporate Europe Observatory (Belgique) et LobbyControl (Allemagne) redoutent que les lobbys affaiblissent cette mise en oeuvre.

De nombreux détails "doivent être clarifiés (...), par exemple en ce qui concerne les normes, les seuils ou les obligations de transparence. La composition du conseil consultatif de la nouvelle agence européenne pour l'IA reste également floue", ont-ils averti.

Les 27 États de l'UE devraient approuver le texte en avril avant que la loi ne soit publiée au Journal officiel de l'UE en mai ou juin.

Risquées, les armes contrôlées par l'IA? Ce qu'il faut savoir

Kathleen Couillard – Agence Science-Pressé (www.sciencepresse.qc.ca)

Mardi 7 novembre 2023

Les avancées de l'intelligence artificielle (IA) ouvrent de nouvelles possibilités dans le domaine militaire, pour la création de ce qu'on appelle des armes autonomes. Faut-il s'en inquiéter?

Qu'est-ce qu'un « système autonome » ?

Un système est appelé « autonome » si, à partir du moment où il est activé, il fonctionne seul, sans intervention humaine. Il peut s'agir autant d'un système simple comme un grille-pain, que du pilote automatique d'un avion, anticipait en 2016 Paul Scharre, auteur d'un rapport du Center for a New American Security sur le risque opérationnel des armes autonomes. Les voitures « sans conducteur » que l'on nous promet depuis une dizaine d'années, entrent aussi dans cette catégorie.

Où en sont les armes autonomes ?

Les systèmes autonomes ont plusieurs applications dans le domaine militaire, observaient des chercheurs du Massachusetts Institute of Technology (MIT) dans un article de 2022. Par exemple, ils peuvent être utiles pour nettoyer un champ de mines ou pour approvisionner les troupes. Mais l'article s'intéressait plus particulièrement aux armes autonomes létales, dans le contexte du développement de l'intelligence artificielle. Et on en parlait depuis longtemps: dès 2016, Paul Scharre entrevoyait que cette automatisation des armes leur permettrait d'être plus précises et de limiter, en théorie, les dommages collatéraux chez les civils.

De fait, les armes autonomes existent depuis longtemps, rappelait en 2022 Neil Davison, conseiller scientifique et politique principal au Comité international de la Croix-Rouge. Il donnait en exemple les systèmes aériens de défense contre les missiles ou les drones kamikazes, qui sont conçus pour voler au-dessus d'un champ de bataille et détruire certaines cibles prédéterminées —comme des radars ou des chars d'assaut. Dans un texte d'opinion publié en 2018 dans la revue *Foreign Policy*, Paul Scharre estimait qu'au moins 30 pays utilisaient déjà des armes autonomes pour défendre leurs bases, leurs véhicules et leurs navires.

L'ajout de l'intelligence artificielle

L'essor de l'intelligence artificielle (IA) ces dernières années a donc ouvert de nouveaux horizons. L'IA, soulignaient les chercheurs du MIT, permet notamment de concevoir des systèmes avec une vitesse de réaction encore plus grande qu'avec les systèmes informatiques d'avant. Les armes contrôlées par l'IA peuvent également

continuer de fonctionner même si elles ne sont plus en mesure de communiquer avec leur base.

À l'heure actuelle, l'IA est utilisée surtout pour ces drones kamikazes et pour des véhicules aériens sans pilote. Par ailleurs, dès le début des années 2010, la division militaire du géant sud-coréen Samsung a développé des fusils sentinelles (*sentry gun*), capables de reconnaître des cibles humaines puis de tirer sur elles. Dans la même décennie, Israël aurait déployé ce type d'arme à sa frontière avec Gaza.

Les risques d'erreurs d'une arme autonome

C'est évidemment arrivé à ce stade que les systèmes autonomes utilisés à des fins militaires deviennent dangereux, s'ils ne fonctionnent pas comme ils le devraient. C'est ce qui était survenu en 2003 au-dessus de l'Irak, rappelle la journaliste spécialisée en technologies militaires Kelsey Atherton. Le système antimissile américain Patriot avait alors abattu par erreur un avion de combat britannique, tuant ses deux pilotes. L'ordinateur du Patriot avait conclu par erreur qu'il s'agissait d'un missile irakien et avait recommandé de faire feu.

Même si ce système n'était pas à proprement parler « autonome », puisque la décision finale de tirer revenait aux humains, sa capacité à traiter des données avec une grande rapidité était déjà de très loin supérieure aux capacités humaines. Vingt ans plus tard, on a atteint un niveau que peu imaginaient en 2003. Et pourtant, beaucoup de choses, aujourd'hui encore, peuvent amener les armes autonomes à se tromper ou à agir de façon imprévisible.

- **Erreurs de programmation ou de conception du logiciel**

Dans son rapport publié en 2016, Paul Scharre rappelait les résultats d'une étude qui avait conclu qu'on trouve en moyenne de 15 à 50 erreurs par 1000 lignes de code dans un logiciel. Si les programmeurs sont très rigoureux, ce taux peut diminuer jusqu'à 0,1. Dans un système composé de millions de lignes de code, cela laisse inévitablement des erreurs.

- **Problèmes lors de la collecte de données**

Dans la masse de données qu'utilise l'IA pour prendre une décision, la qualité de ces données peut faire une différence, peut-on lire dans un rapport de l'Institut des Nations unies pour la recherche sur le désarmement, publié en 2021. Or, en contexte de guerre, la qualité des données peut être problématique: une mauvaise ligne téléphonique ou une connexion satellite instable, des senseurs mal calibrés, la fumée qui nuit à la visibilité, etc.

De plus, le risque d'erreur augmente si l'IA a été entraînée avec des données qui ne correspondent pas à celles recueillies dans les conditions de combat, souligne Kelsey Atherton. Par exemple, le système Patriot, en 2003, avait été conçu en présumant qu'il devrait réagir à un nombre important de missiles. Or, pendant son premier mois d'opération, au tout début de la guerre en Irak, il a plutôt été exposé à 41 000 avions alliés et à seulement 9 missiles balistiques irakiens.

- **Cyberattaques**

S'ajoute à cela le fait que les systèmes militaires sont utilisés contre des adversaires qui ont tout intérêt à corrompre les données. C'est d'autant plus préoccupant que l'IA est facile à tromper. Dans une expérience réalisée en 2021 par la compagnie OpenAI, le simple fait de coller une étiquette avec le mot « iPod » sur une pomme amenait le logiciel à l'identifier comme un iPod avec un niveau de confiance de 99,7 %. Une autre expérience menée en 2018 a réussi à rendre un panneau d'arrêt indétectable en lui ajoutant des autocollants.

- **Interactions non prévues avec l'environnement**

Paul Scharre donne aussi l'exemple de huit avions déployés dans le Pacifique en 2007. Lorsqu'ils ont traversé la ligne de changement de date, cela a provoqué un arrêt immédiat des systèmes informatiques. Ce bogue n'avait pas été identifié à l'étape des tests du système.

Les risques d'escalade

Tous les systèmes autonomes —militaires ou non— comportent des risques. Les dérapages des agents conversationnels dans la dernière année —ceux qui, par exemple, insèrent de fausses informations dans des textes— le rappellent aussi. Mais le potentiel de dommages est différent avec une arme, et pas uniquement parce que des vies humaines sont en jeu. Un soldat peut lui aussi se tromper et viser la mauvaise cible, mais le risque que plusieurs soldats fassent exactement la même erreur en même temps à plusieurs reprises, est faible. La machine autonome, elle, pourrait effectivement répéter la même erreur jusqu'à ce qu'elle soit mise hors fonction. Dans un contexte politique tendu, prévient Neil Davison, les armes autonomes pourraient accélérer l'utilisation de la force et augmenter le risque d'escalade d'un conflit.

En raison de la rapidité de l'IA, il est difficile de prévoir combien de temps mettraient les humains avant d'intervenir. En 2018, Paul Scharre faisait un parallèle avec les algorithmes utilisés sur les marchés boursiers, qui prennent des décisions en quelques microsecondes, ce qui peut représenter plusieurs millions de dollars de transactions. Scharre citait aussi le Secrétaire à la défense des États-Unis Robert Work qui, deux ans plus tôt, avait résumé le problème ainsi: « si nos adversaires vont vers des Terminators, et qu'il s'avère que les Terminators sont capables de prendre des décisions plus vite, même si elles sont mauvaises, comment réagirons-nous? »

Plus tôt cette année, le *New York Times* donnait la parole à des membres de la communauté militaire inquiets, dans un contexte où des réglementations sur l'IA se font attendre: « personne ne sait vraiment de quoi ces technologies sont capables lorsqu'il est question de développer et de contrôler des armes » et personne n'a la moindre idée « du type de régime de contrôle des armes qui pourrait fonctionner ».

Une complexité difficile à saisir

Plus un système est complexe, plus il est difficile pour son opérateur de le comprendre. La complexité d'un système affecte donc la capacité de l'humain à en prévoir le comportement.

Rappelons à ce sujet que les armes autonomes contrôlées par l'intelligence artificielle se basent sur ce qu'on appelle l'apprentissage machine (*machine learning*). En d'autres

mots, rappelle Neil Davison, ces logiciels s'écrivent eux-mêmes grâce à la grande quantité de données qui leur est fournie pour s'entraîner. Cela signifie que même le programmeur n'en connaît pas la structure interne et peut donc difficilement prédire son comportement.

Dans certains cas, l'humain pourrait même ne pas être en mesure de réaliser que le système se trompe. Déjà en 2003, les soldats qui utilisaient le système Patriot n'étaient pas en mesure de déterminer si les informations fournies par le système étaient pertinentes. Ils lui ont donc fait confiance et ont accepté sa recommandation de faire feu.

Verdict

Les armes autonomes contrôlées par l'IA existent d'ores et déjà, et en dépit des progrès des dernières années, il est acquis qu'elles peuvent encore faire des erreurs. De plus, le potentiel de dommages élevé est inhérent à la nature même de ces systèmes: leur rapidité, qui constitue leur principal attrait aux yeux des militaires, et leur complexité.

L'INTELLIGENCE ARTIFICIELLE ET LE MONDE DE LA DÉFENSE

www.entreprises.gouv.fr / juin 2023

Depuis plusieurs années déjà, le ministère des Armées développe ses relations avec la communauté scientifique française en intelligence artificielle et soutient des travaux qui pourront être à l'origine de nouvelles technologies d'intérêt pour la Défense.

L'Intelligence Artificielle (IA) est une technologie d'intérêt dual, qui trouve bon nombre d'applications dans les systèmes de défense (navigation autonome, planification, aide à la décision, santé du soldat, etc.). C'est pourquoi, depuis plusieurs années déjà, le ministère des Armées développe ses relations avec la communauté scientifique française en IA et soutient des travaux qui pourront être à l'origine de nouvelles technologies d'intérêt pour la Défense. Le recours à l'IA au ministère des Armées **nécessite la maîtrise de la donnée et de son exploitation**. La donnée est massive, très variée et produite parfois par des grands capteurs spécifiques au monde de la défense comme les sonars ou les radars par exemple. Dans un contexte opérationnel, elle peut nécessiter une mise à jour vélocité et sa véracité ne doit pas pouvoir être mise en doute. Enfin, il faut pouvoir la capter, la traiter et la valoriser dans ces nouveaux systèmes. Elle constitue un point de passage obligé de l'IA et un facteur de « durcissement » des applications d'IA dans le monde militaire.

Enfin, notre pays se veut être un modèle d'utilisation maîtrisée de l'intelligence artificielle. À ce titre, la recherche d'une IA de confiance est un objectif clé pour assurer la robustesse et la compatibilité des applications avec les contraintes du monde de la défense, en particulier la criticité de ses fonctions. Par ailleurs, l'application de l'IA soulève la question de l'éthique. Pour respecter un haut niveau éthique, la France a choisi de **maintenir systématiquement la responsabilité du commandement militaire dans l'emploi des armes**. Pour atteindre ces objectifs, le ministère des Armées s'est doté d'un comité d'éthique, installé en 2020.

En résumé, pour la Défense, le développement de l'IA a pour objectif **d'accroître significativement l'autonomie stratégique et la supériorité opérationnelle et technologique de nos armées**.

OBJECTIFS

- Répondre aux enjeux opérationnels en appliquant l'IA dans les domaines prioritaires du ministère.
- Optimiser le traitement des données liées aux capteurs spécifiques défense (radars, sonars, équipements de guerre électronique, etc.).
- Préparer les missions en amont (simulateurs plus immersifs et performants, planification, etc.).
- Favoriser les déclinaisons opérationnelles des travaux de R&T en IA.

CHIFFRES CLÉS

- Budget : 100 millions d'€/an en moyenne sur la période LPM (Loi de programmation militaire) 2019-2025 pour les études et la recherche sur l'IA
- Recrutement de 200 spécialistes de l'IA d'ici 2023
- 5 acteurs autour de l'IA de Défense : DGA (Direction générale de l'Armement), SGA, DGRIS, EMA et AID (Agence de l'innovation de la défense)

L'ONU veut réguler l'intelligence artificielle militaire mais se heurte au principe de réalité concurrentielle

par THIERRY BERTHIER

Revue CONFLITS – Août 2023

L'ONU a exprimé son désir de bannir l'usage de l'IA dans les armes de guerre autonomes à l'horizon 2026 et de réguler l'IA militaire à l'échelle mondiale. Antonio Guterres s'est dit favorable à la création d'un conseil spécifique à l'IA, ayant pour objectif d'aider à réguler, gérer l'usage de l'IA militaire et règlementer ses dérives potentielles.

La première réunion du conseil de sécurité de l'ONU dédiée à l'Intelligence Artificielle (IA) a eu lieu le 18 juillet 2023. Le Secrétaire Général des Nations Unies, Antonio Guterres a souligné les progrès spectaculaires de l'intelligence artificielle et de ses applications potentielles au bénéfice du développement commun, du recul de la pauvreté, de l'éducation, de l'industrie, de l'agriculture et de la résolution des grands problèmes environnementaux.

Il a également exprimé son désir de bannir l'usage de l'IA dans les armes de guerre autonomes à l'horizon 2026 et de réguler l'IA militaire à l'échelle mondiale. Selon lui, « *l'utilisation malveillante de systèmes d'IA à des fins terroristes criminelles ou étatiques pourrait entraîner un nombre effroyable de morts et de destructions, des traumatismes généralisés et des dommages psychologiques profonds à une échelle inimaginable* ». Ce constat posé, Antonio Guterres s'est dit favorable à la création d'un conseil spécifique à l'IA, ayant pour objectif d'aider à réguler, gérer l'usage de l'IA militaire et règlementer ses dérives potentielles.

La réunion dirigée par Antonio Guterres a donné lieu aux premières recommandations exprimées par certains membres de l'ONU montrant une volonté forte de régulation et d'interdiction future des systèmes armés autonomes.

Il faut tout d'abord saluer l'initiative du Conseil de Sécurité et l'organisation de cette réunion inaugurale car les révolutions IA-robotique vont transformer en profondeur l'ensemble des activités humaines. Il est donc important que les grandes puissances et les puissances secondaires puissent échanger librement au sein de l'ONU, et débattre sur les enjeux et les défis de l'IA.

Le volet militaire de l'IA nous fait a priori passer du « côté obscur de la Force ». La réunion dirigée par Antonio Guterres a donné lieu aux premières recommandations exprimées par certains membres de l'ONU montrant une volonté forte de régulation et d'interdiction future des systèmes armés autonomes. Les trois premières puissances militaires (USA, Chine et Russie) ont indiqué, l'une après l'autre, qu'elles se réservaient

le droit de développer des systèmes d'armes intégrant de l'IA tout en précisant que ces systèmes devaient rester sous le contrôle humain. Derrière ces premières déclarations, il faut comprendre qu'aucune de ces trois puissances dominantes n'a l'intention de signer un texte limitant l'usage de l'IA militaire ni de freiner ses investissements massifs (en dizaines de milliards de dollars) réalisés au titre de la recherche et du développement.

1 – Les quatre principes de réalité systémique de l'IA

Concrètement, la déclaration du Secrétaire Général de l'ONU sur l'IA militaire se heurte à quatre grands principes de réalité systémique associés à la diffusion et à l'usage du progrès technologique au bénéfice des activités humaines, civiles et militaires :

Principe n°1 : Le principe du sens unique temporel ou de non-retour en arrière face à une avancée technologique majeure, accessible, impactante et à fort pouvoir libérateur.

Principe n°2 : Le principe de diffusion maximale d'une technologie duale (ayant des applications à la fois civiles et militaires) ;

Principe n°3 : Le principe d'appropriation maximale des technologies efficaces dans un contexte de compétition mondiale et de concurrences géopolitiques.

Principe n°4 : Le principe d'emploi maximal de technologies apportant un avantage tactique ou stratégique sur un adversaire en contexte de guerre ou de guerre froide.

2 – L'intelligence artificielle comme moteur de la haute intensité du combat

Les applications militaires de l'intelligence artificielle s'inscrivent dans toute la largeur du spectre opérationnel et renforcent les dynamiques de haute intensité au combat

- **Renseignement :** collecte, traitement et analyse automatique des données, images satellitaires, imagerie drones, analyse de documents, traduction automatique, localisation, contextualisation à partir d'images, veille documentaire.
- **Logistique :** préparation de missions, OPEX, aide au dimensionnement du dispositif, préparation du soutien, optimisation des approvisionnements (carburants, vivres, eau, munitions).
- **Simulation :** simulation de déploiement, wargame, test d'hypothèses et de capacités, simulation de déploiement d'unités robotisées, entraînement des troupes au combat, entraînement sur de nouveaux systèmes d'armes.
- **Conduite des opérations, IA C2 :** Aide à la décision pour les centres de commandement et contrôle (IA C2), reporting, tests et validation d'hypothèses de manœuvres, tests d'impact et d'attrition au regard de l'intensité du combat
- **Systèmes robotisés armés :** Augmentation du niveau d'autonomie des systèmes, escadrilles et essaims de drones aéroterrestres, marins, sous-marins.

Systemes et boucliers anti-missiles autonomes, systemes radars intelligents, Lutte Anti-Drones par essais de drones anti-drones, Niveaux d'autonomie L0,L1,...L5

- **Cybersécurité et cyberdéfense** : Emploi de l'IA pour sécuriser les applications, systemes d'information et systemes d'armes, SIEM UEBA (User and Entity Behavior Analytics (UEBA) and Security Information and Event Management (SIEM)), détection et remédiation automatique des attaques, maitrise du risque cyber. Opérations cyber offensives soutenues par l'IA.
- **PsyOps, opérations cognitives, ingérence et contre-ingérence** : détection et remédiation des opérations d'influence, de fracturation des opinions, d'atteinte à l'image, de campagnes de FakeNews produites à partir des réseaux sociaux (fermes de bots), production d'ADFI (Architectures de Données Fictives Immersives) utilisées pour tromper ou influencer une cible.

3 – Les grands défis de l'IA militaire

La robotisation du champ de bataille, la préservation du sang du soldat humain, la réduction temporelle des toutes les étapes de la boucle OODA [O – Observe (observer), O – Orient (orienter), D – Decide (décider), A – Act (agir)], et la recherche de haute intensité au combat sont des objectifs prioritaires pour toutes les armées du monde. Chacun de ces objectifs s'appuie sur les progrès des sciences et technologies, en particulier sur ceux de l'intelligence artificielle qui apporte l'autonomie, la précision et la vitesse de réaction dans les systemes. Si les défis de l'IA militaire sont multiples, deux d'entre eux apparaissent désormais comme prioritaires en retour d'expérience notamment de la guerre russo-ukrainienne :

Défi n°1 – l'IA-C2 (Command & Control) : l'IA intégrée au sein du systeme de commandement permet de prendre en compte l'ensemble des données qui remontent du terrain, du renseignement, des capteurs déployés, des unités à engager ou déjà engagées. L'apport de l'IA réside dans sa capacité à tester des hypothèses de manœuvre, à en mesurer les effets sur l'ennemi et sur ses forces, à évaluer le risque associé à une action militaire. La simulation numérique intégrant de l'apprentissage automatique et de l'apprentissage par renforcement donne la possibilité de jouer une séquence opérationnelle, de modifier ses paramètres, de rejouer la séance et de converger vers une solution optimale pour le chef militaire qui en tient compte dans son arbitrage.

Défi n°2 – l'IA embarquée dans les escadrilles et essais de robots aéroterrestres : La guerre russo-ukrainienne est une guerre des drones aériens vecteurs d'une très forte attrition sur les chars et blindés des deux belligérants. Les premières escadrilles de munitions téléopérées navales ont été déployées par l'armée ukrainienne contre les navires russes. Des drones kamikazes sont régulièrement utilisés dans la profondeur par les deux armées. Ainsi, la question de la lutte anti-drones (LAD) devient prioritaire tout en restant techniquement complexe. L'avantage restant à l'attaquant, le défi de la LAD repose avant tout sur les capacités de détection, de suivi et de neutralisation des vecteurs ennemis. L'intelligence artificielle apporte des solutions très prometteuses pour contrer l'attaque d'un essaim aérien constitué de plus de 100

drones. La méthode de LAD consiste à mettre en œuvre un essaim de drones aérien « anti-essaim » composé lui aussi de plus de 100 drones « racers » qui vont chacun suivre un vecteur ennemi et le détruire par choc cinétique ou par détonation via une charge embarquée. L'action globale de l'essaim anti-essaim ne peut être dirigée que par l'intelligence artificielle.

Ces deux défis, qui reposent pleinement sur les progrès de l'IA, font l'objet d'investissements en R&D très conséquents (plusieurs dizaines de Milliards de dollars) en Chine et aux Etats-Unis. La course à la haute intensité et aux missiles hypersoniques repose elle aussi sur les apports de l'IA militaire. On comprend facilement que ni la Chine ni les Etats-Unis n'accepteront de limiter ou de renoncer à la course à « l'Armement » si déterminant dans la recherche de puissance et d'ascendant sur l'ennemi. Le Secrétaire Général de l'ONU mesure parfaitement l'importance des enjeux géopolitiques qui accompagnent le développement de la robotique militaire. Il aura par contre toutes les difficultés à obtenir un moratoire ou un encadrement sur ce type d'armes.