De l'Ukraine à Gaza : l'Intelligence artificielle en guerre

Par **Amélie Férey** et **Laure de Roucy-Rochegonde**

Amélie Férey coordonne le Laboratoire de recherche sur la défense de l'Ifri.

Laure de Roucy-Rochegonde est responsable du Centre Géopolitique des technologies de l'Ifri.

Les guerres en Ukraine et à Gaza témoignent d'une forte pénétration de l'Intelligence artificielle (IA) sur le champ de bataille. Les usages de cette technologie sont nombreux, de l'analyse du renseignement au ciblage, en passant par la logistique ou la communication. Le rythme des opérations s'accélère tellement que le temps laissé aux humains pour prendre des décisions de tir se réduit à quelques secondes. Pour enrayer cette spirale, les applications militaires de l'IA doivent être régulées.

politique étrangère

Dans un article paru au printemps 2024 dans *Defense One*[1], le stratégiste américain Peter Singer compare les conflits actuels à la guerre civile espagnole. En 1936, explique-t-il, les deux camps utilisaient des fusils et creusaient des tranchées. Cependant, arrivaient au même moment sur le champ de bataille le char d'assaut, la radio et l'avion. Ce n'est donc pas parce que les belligérants recourent à des méthodes éprouvées qu'une rupture ne peut concomitamment survenir. En réalité, conclut-il, les guerres en cours en Ukraine et à Gaza, tels des laboratoires des conflits futurs, en disent davantage sur la guerre *qui vient*, à l'image de ce qu'annonçait la guerre d'Espagne pour la Seconde Guerre mondiale. Or, parmi les développements technologiques observés sur ces deux théâtres, le recours massif à l'Intelligence artificielle (IA) est probablement celui qui suscite le plus de surprise et de questions.

Apparue en 1965 dans les travaux du logicien John McCarthy, l'expression « Intelligence artificielle » renvoie à l'ensemble des théories et

1. P. Singer, « The AI Revolution is Already Here. The U.S. Military must Grapple with Real Dilemmas that until Recently Seemed Hypothetical », *Defense One*, 14 avril 2024.

techniques visant à mieux comprendre les intelligences humaines, et à les imiter à l'aide de programmes informatiques qui simulent leur fonctionnement. Dans un sens plus générique, l'IA qualifie la capacité de systèmes à accomplir des tâches requérant normalement un raisonnement humain.

Cette technologie n'en finit plus de s'immiscer dans nos vies personnelles et professionnelles, *a fortiori* depuis le succès commercial de l'agent conversationnel ChatGPT développé par OpenAI et le boom des IA génératives, c'est-à-dire capables de créer des contenus inédits à partir de jeux de données préexistantes. Sur le champ de bataille comme ailleurs, les promesses de l'IA attisent les convoitises et les innovations se multiplient, ce qui n'est pas sans poser de nombreuses questions en matière de stratégie, de politique, de droit et d'éthique.

Les applications militaires de l'IA sont nombreuses et protéiformes. De la logistique au ciblage en passant par le renseignement et l'aide à la décision au sein des fonctions de commandement et de contrôle, l'IA irrigue désormais l'intégralité des systèmes de force contemporains. Elle est même envisagée comme une nouvelle révolution des techniques de la guerre, au même titre qu'avant elle la poudre à canon ou l'arme nucléaire.

Depuis une dizaine d'années, les progrès de l'IA militaire sont exponentiels, tant les grandes puissances ont pris conscience du potentiel que celle-ci revêt. Elle présente en effet des avantages déjà largement démontrés, qui peuvent prendre de multiples formes différentes : l'IA est intégrée, entre autres, dans les munitions rôdeuses, dans les drones aériens, terrestres et maritimes, dans les sentinelles stationnaires, dans les systèmes de lutte antidrones ou encore dans les systèmes de défense antiaérienne. Au-delà du seul spectre des « robots tueurs », il convient donc de réfléchir aux conséquences de l'arsenalisation de l'IA : celle-ci est-elle susceptible de transformer la nature de la guerre ?

L'IA est identifiée depuis plus d'une décennie comme un « multiplicateur de force » par le département de la Défense américain. Si son développement militaire s'inscrit dans une trajectoire historique et conceptuelle déjà longue, l'analyse du recours à l'IA par les armées ukrainienne et israélienne démontre combien cette technologie change la donne sur les théâtres d'opérations. Tandis que Tsahal investit depuis des années dans le développement de l'IA militaire et l'utilise désormais pour asseoir sa supériorité technique face aux combattants du Hamas, en Ukraine, elle sert le faible au détriment du fort, par l'intégration en temps réel des briques technologiques indispensables à la lutte contre le mastodonte

russe. Ces nouveaux usages s'accompagnent toutefois d'un contrôle humain de plus en plus réduit.

Les promesses de l'IA militarisée

Selon le stratège américain Andrew Marshall, la « révolution dans les affaires militaires » consiste en un bouleversement radical de l'art de la guerre et de la conduite des opérations, du fait de l'introduction de nouvelles technologies. L'IA et les applications qui y sont associées s'inscrivent dans cette logique.

L'augmentation du nombre de capteurs, c'est-à-dire de tout appareil de collecte de l'information – des boules optroniques présentes sur les drones aériens jusqu'au smartphone d'un civil –, sont autant de sources d'information localisées sur le champ de bataille mais également sur le territoire de n'importe quel pays, ami, ennemi ou neutre. Ils collectent un nombre colossal de données hétérogènes, que l'IA croise et analyse. Les officiers peuvent alors en tirer parti et prendre des décisions plus informées sur le champ de bataille – qui devient de ce fait plus « transparent ».

L'IA est indispensable au regard de l'accélération du rythme des opérations

L'IA permet en outre de qualifier les données collectées en les rattachant à une cible ; par les signatures radar, électromagnétiques, mais aussi par la reconnaissance d'images ou par l'identification de « conduites récurrentes » de la part d'ennemis facilitant leur identification – ce qu'on appelle en anglais des *patterns of life*. La décision de faire feu peut dès lors être prise plus rapidement par une accélération de la boucle *observe, orient, decide and act* (*OODA loop*), car les capteurs détectant une cible sont directement reliés à des officiers par le biais d'une connectivité accrue et d'une mise en réseau des différents appareils et centres de commandement. Ainsi l'intégration de l'IA dans les systèmes d'armes permet-elle de faire face à des situations opérationnelles qui combinent un rythme rapide, un environnement complexe et une grande quantité d'objectifs. L'IA est alors indispensable au regard de l'accélération du rythme des opérations, qui semble vouée à s'accentuer, si l'on en croit les prédictions[2] du général John Allen en 2017 sur l'*hyperwar*.

L'intégration de techniques d'IA aux systèmes d'armes fait enfin apparaître la possibilité d'essaims de robots. Ceux-ci fonctionnent grâce au calcul déporté, distribué et miniaturisé, permettant à des vecteurs

2. J. R. Allen et A. Husain, « On Hyperwar », *Proceedings*, vol. 143, nº 373, 2017.

– principalement des drones – de communiquer à faible distance et à haut débit entre eux, tandis qu'ils opèrent à faible débit et à grande distance de leur opérateur. L'IA rend possible l'émergence d'une manœuvre propre en réduisant le lien avec l'opérateur au sol, qui laisse l'essaim définir lui-même le meilleur mode d'action.

À titre d'exemple, lors de l'opération Gardiens des murs, à Gaza au printemps 2021, l'armée israélienne a utilisé un essaim de petits drones multicoptères pour localiser, identifier et cibler des membres du Hamas. Bien qu'il s'agisse vraisemblablement de la première utilisation d'un essaim de drones au combat, l'essai s'est avéré si efficace que Tsahal a immédiatement annoncé sa volonté de le déployer dans d'autres unités. Une compagnie de soutien de sa brigade des parachutistes aurait ainsi été dotée d'une unité d'essaim de drones. Leur commandant a affirmé que celle-ci avait mené plus d'une trentaine d'opérations réussies, y compris contre des cibles à plusieurs kilomètres de la frontière entre Gaza et Israël[3].

D'un point de vue militaire, de telles capacités sont éminemment avantageuses pour affronter un adversaire et le forcer à répondre à de multiples menaces à la fois. Les essaims de drones ouvrent des perspectives prometteuses en termes de masse, de discrétion, de furtivité et de saturation. Ils multiplient les charges utiles tout en diminuant le nombre d'opérateurs humains, ce qui les rend très intéressants sur le plan économique. De plus, leur grande autonomie et l'allocation dynamique des tâches les rendent résilients à la lutte antidrones.

En Ukraine : du faible au fort

The First AI War : c'est ainsi que le magazine américain *Time* présentait la guerre russo-ukrainienne en couverture de son numéro du 26 février 2024. Avant l'invasion de l'Ukraine le 24 février 2022, la Russie était considérée comme l'une des puissances militaires les plus avancées en matière d'arsenalisation de l'IA, du fait de ses nombreuses expérimentations sur les terrains ukrainien et syrien. Contre toute attente, c'est l'armée ukrainienne qui s'est démarquée par son utilisation d'armes dopées à l'IA.

Du point de vue ukrainien, en effet, l'avantage quantitatif russe peut être compensé par des solutions technologiques accroissant l'efficacité des opérations militaires. Cette stratégie de nivellement vise explicitement à prendre l'avantage grâce à l'innovation. D'après l'hebdomadaire *Dzerkalo*

3. Z. Kallenborn, « Israel's Drone Swarm Over Gaza Should Worry Everyone », *Defense One*, 7 juillet 2021, disponible sur : www.defenseone.com.

Tyjnia, l'utilisation de l'IA par l'armée ukrainienne se décline désormais en dix domaines différents : l'autonomie des systèmes d'armes, l'observation et la reconnaissance, l'identification et la classification des cibles, l'analyse et la prédiction des menaces, la logistique et le ravitaillement, la cybersécurité, la guerre électronique, la simulation et la formation, la santé des armées et l'aide à la décision.

Ce nouvel arsenal s'observe en premier lieu dans la place occupée par les systèmes téléopérés dans le conflit. L'annexion de la Crimée en 2014 avait déjà montré combien les drones étaient vulnérables aux techniques de brouillage. Le recours à l'IA permet dès lors de pallier la perte de liaison entre un système d'armes et son opérateur, et de poursuivre la mission dans un environnement électromagnétique contesté. L'IA démultiplie les capacités de guerre électronique, tout en améliorant la réponse aux vulnérabilités qu'elles engendrent.

Confronté à un adversaire supérieur en nombre et en armement, Kiev compense son infériorité par le déploiement massif de drones. Or ceux-ci ont la particularité de n'être pas seulement des effecteurs, mais aussi des capteurs. Les données recueillies par ces drones intelligents doivent donc être traitées, ce qui s'avère extrêmement chronophage. À titre de comparaison, rien qu'en 2009, les drones américains déployés en Afghanistan et en Irak avaient enregistré un nombre si important d'images que la CIA avait estimé que vingt-quatre années seraient nécessaires pour les visionner en intégralité. Là encore, les techniques d'IA permettent d'agréger ces données parfois très hétérogènes pour en tirer des recommandations, notamment en termes de ciblage.

Kiev compense son infériorité par le déploiement massif de drones

L'un des rôles clés de l'IA en Ukraine est justement d'intégrer de la reconnaissance de cibles et d'objets à l'imagerie satellite. L'objectif est de géolocaliser et d'analyser des données de source ouverte, telles que les contenus des réseaux sociaux, afin d'identifier les soldats russes, les armes, les systèmes, les unités ou leurs mouvements. Les réseaux neuronaux sont utilisés pour combiner des photographies au niveau du sol, des séquences vidéo provenant de drones ainsi que des images satellite, permettant d'accélérer l'analyse et l'évaluation du renseignement puis de générer des avantages stratégiques et tactiques[4].

4. S. Bendett, « Roles and Implications of AI in the Russian-Ukrainian Conflict », Center for a New American Security, 20 juillet 2023.

Les Ukrainiens n'ont toutefois pas relevé seuls le défi de l'arsenalisation de l'IA dans leur guerre contre la Russie. Ils ont été soutenus par bon nombre de géants technologiques américains. Le PDG de Palantir, Alex Karp, s'est rendu à Kiev dès juin 2022 pour proposer gratuitement ses services au président Volodymyr Zelensky[5]. À sa suite, Microsoft, Amazon, Google ou encore Starlink ont afflué en Ukraine, où ils ont pu expérimenter leurs systèmes d'IA appliqués au renseignement et au combat. L'armée ukrainienne utilise ainsi le système Skykit, développé à l'aide du logiciel MetaConstellation de Palantir. À la manière d'un centre de renseignement mobile, Skykit analyse des images satellite et élabore des plans de frappe pouvant être conduits sans contact avec la chaîne de commandement.

Derrière ce volontarisme des *Big Tech* américaines se cachent des intérêts bien compris. D'abord, le fait de voler au secours des Ukrainiens a permis à un certain nombre d'entreprises aux méthodes controversées – à l'image de Palantir ou Clearview AI[6] – de redorer un blason entaché de soupçons de surveillance de masse. Dans le même temps, elles ont pu capitaliser sur une manne de données opérationnelles, qui étaient précisément celles qui manquaient pour rendre plus robustes les applications militaires de l'IA. En intégrant rapidement les retours d'expérience du terrain, elles ont également pu innover promptement et améliorer leurs modèles en temps réel. Enfin, ces nouveaux systèmes *combat proven* sont promis à de lucratifs débouchés commerciaux : le label « expérimenté en Ukraine » est devenu un argument marketing, comme l'a montré le salon de l'armement Eurosatory qui s'est tenu du 17 au 21 juin 2024.

À Gaza : du fort au faible

Depuis 2017, l'armée israélienne envisage l'IA comme la « clé de la survie moderne ». En 2018, elle annonçait avoir développé des machines « dépassant l'IA » et, deux ans plus tard, actait le rôle de l'IA comme clé de l'innovation militaire dans son plan de modernisation Momentum. Dès 2021, elle qualifiait l'opération Gardiens des murs de « première guerre de l'IA ».

Cette volonté de miser sur l'IA pour acquérir une supériorité militaire s'incarne dans l'utilisation de différents logiciels. Les plus connus sont

5. V. Bergengruen, « How Tech Giants Turned Ukraine Into an AI War Lab », *Time*, 8 février 2024.
6. Clearview AI est une entreprise spécialisée dans la reconnaissance faciale assistée par IA, qui a été critiquée pour avoir recueilli ses données en extrayant des milliards de photographies publiques sur internet, en violant les droits à la vie privée et en vendant l'accès aux forces de l'ordre. En Ukraine, elle a notamment permis aux forces ukrainiennes d'identifier des centaines de milliers de soldats russes. V. Bergengruen, « Ukraine's "Secret Weapon" Against Russia Is a Controversial U.S. Tech Company », *Time*, 14 novembre 2023.

Depth of Wisdom, cartographiant la bande de Gaza afin d'y déceler les tunnels du Hamas, et Habsora, qui identifie les bâtiments pouvant par exemple servir de sites militaires pour le lancement de roquettes, l'entraînement ou encore entreposer des armes.

Plus récemment, le journal d'investigation +972 a décrit le fonctionnement de deux autres logiciels, Lavender et Where's daddy?. Lavender mesure le taux de probabilité qu'a un Gazaoui de faire partie d'une organisation armée, en comparant ses schémas de communication (changement régulier de numéro de téléphone, contacts avec des numéros affiliés à ces organisations, etc.) à ceux de membres avérés du Hamas ou du Djihad islamique. Where's daddy?, quant à lui, localise les personnes ciblées lorsqu'elles rentrent à leur domicile puis alerte les officiers de leur présence dans les bâtiments identifiés pour que ces derniers puissent faire feu, et ce malgré la présence de civils.

Cette utilisation de l'IA s'appuie donc sur un système de surveillance de masse, permettant par la collecte d'un volume considérable de données d'entraîner les algorithmes, en agrégeant les données de communication avec celles provenant de satellites, de drones, de caméras de vidéosurveillance ou encore des réseaux sociaux.

Ce pari fait sur l'IA militaire s'est révélé désastreux dans l'opération Glaive de fer. Tsahal a en effet combiné au moins trois séries d'erreurs. Elle a d'abord mal paramétré ses algorithmes, avec un jeu de données qui n'était pas robuste : les données de communication utilisées pour repérer les membres du Hamas – par exemple le fait qu'ils changeaient régulièrement de téléphones – étaient également des pratiques adoptées bien plus largement par des militants de défense des droits de l'homme, des journalistes, mais aussi par des personnes déplacées à cause des bombardements et qui ramassaient des téléphones trouvés çà et là pour contacter leurs familles. Autre erreur : le biais de « surconfiance » dans la rationalité des algorithmes. Dans les jours qui ont suivi le 7 octobre, face à l'émotion de la société israélienne, les pressions pour frapper vite et fort ont été maximales. Les vérifications humaines des prescriptions des logiciels ont donc été réduites *a minima*, un officier passant vingt secondes à vérifier la validité d'une cible humaine proposée par Lavender, alors même que le taux d'erreur attribué au système était de 10 %. Certaines personnes ont, par exemple, été identifiées comme appartenant au Hamas simplement parce qu'elles portaient le même nom qu'un militant avéré, ou qu'elles étaient dans un groupe WhatsApp commun. Enfin, l'utilisation de l'IA a rationalisé une doctrine de ciblage pour le moins suspecte au regard du droit international, et notamment de son principe de proportionnalité, en autorisant un nombre important de « dommages collatéraux ».

Autre domaine d'utilisation de l'IA qui mérite d'être souligné, la Stratcom israélienne s'est appuyée sur les nouvelles technologies pour produire des images justifiant son opération militaire ainsi que pour amplifier des contenus appuyant son « narratif ». Les images illustrant le poste de commandement du Hamas supposément situé sous l'hôpital Al-Shifa ont, par exemple, semé la confusion entre réalité et fiction. Autre exemple, la vidéo *Come visit beautiful Gaza*, mise en ligne par le National Public Diplomacy Directorate rattaché au Premier ministre israélien, illustre ce qu'aurait pu être Gaza sans le Hamas, en renversant la responsabilité des nombreuses destructions sur le Hamas, et non sur l'armée israélienne. L'IA a également été mise à contribution dans le cadre de manœuvres informationnelles afin d'amplifier des contenus soutenant la communication stratégique israélienne sur les réseaux sociaux, ou pour réprimer des messages pro-palestiniens en scannant les contenus des profils de militants.

De nouvelles menaces

Les perspectives prometteuses offertes par l'intégration de l'IA aux systèmes d'armes s'accompagnent toutefois de nouvelles vulnérabilités, en grande partie liées à l'érosion du contrôle exercé par l'humain sur l'emploi de la force.

Tout d'abord, le recours à des techniques d'IA présente des risques dus à la convergence entre lutte informatique et guerre électronique. En effet, les moyens de guerre électronique permettent d'accéder à des systèmes d'information adverses peu connectés avec l'extérieur. Or un système d'IA étant un système d'information comme un autre, il constitue une voie d'accès électromagnétique par laquelle des données peuvent transiter pour mener une attaque. Leur généralisation risque donc d'étendre la surface de vulnérabilité, à la fois des systèmes et des réseaux dans lesquels ils évoluent[7]. Dans le même temps, l'intégration d'IA rend les systèmes vulnérables aux cyberattaques et au piratage informatique, qui pourraient donner lieu à des opérations de *deception* ou de sabotage – par exemple par l'intoxication des algorithmes grâce à des données altérées. Avec ce type d'attaque informatique, un adversaire pourrait leurrer un drone, voire en prendre le contrôle à distance.

Se pose également la question de la « métacognition », dans l'hypothèse où des systèmes poursuivraient leur apprentissage en cours de mission, afin de s'adapter à des environnements changeants. Sans contrôle efficace,

7. J. Jun, « How Will AI Change Cyber Operations? », *War on the Rocks*, 30 avril 2024.

ce qui serait « appris » par ces systèmes pourrait donner lieu à des réactions inattendues, indésirables et ne correspondant pas au cadre d'emploi prévu. Plus largement, des systèmes auto-apprenants, capables d'évoluer au cours de leur utilisation opérationnelle, poussent à s'interroger, au-delà même de la maîtrise de leur configuration, sur la possibilité d'en garantir la fiabilité dans la durée.

Peuvent enfin être mis en avant les risques de prolifération et de dissémination de ces technologies auprès d'acteurs hostiles. Parce que l'IA permet de réduire la taille et le coût des systèmes d'armes, ainsi que les risques encourus par les forces, tout en améliorant leur productivité et leur sécurité, elle pourrait s'avérer particulièrement dangereuse si des groupes terroristes parvenaient à s'en doter.

La Stratégie française d'Intelligence artificielle de défense mentionne par ailleurs que certaines puissances dites révisionnistes, telles la Russie ou la Chine, considèrent que le *statu quo* international peut être bousculé à leur avantage grâce aux technologies émergentes s'appuyant sur l'IA militaire. Ces dernières permettent une forme de nivellement des positions stratégiques, car elles sont relativement peu coûteuses et aisées à maîtriser. Dans le même temps, d'autres acteurs pourraient « rentrer dans le jeu », en acquérant des technologies qui, bien que complexes, deviennent de moins en moins onéreuses et donc toujours plus accessibles. Cette dissémination permettrait alors aux parties les plus faibles de modifier les équilibres entre elles et leurs adversaires.

Quelle place pour l'humain ?

Au-delà de ces enjeux d'ordre technique, de nouvelles craintes émergent, liées à ce que Peter Singer a décrit[8] comme « le rôle de plus en plus réduit de l'être humain dans la guerre contemporaine ». D'une part, l'accélération du rythme de la guerre et le « déluge de données » qui accompagnent l'arsenalisation de l'IA peuvent nuire au jugement humain, puisque les opérations tendent à devenir trop rapides pour la compréhension humaine. L'opérateur risque d'être « noyé » dans un flot d'informations, incapable d'exercer son entendement compte tenu de la vitesse de réaction du système[9]. L'humain n'est alors plus en position de comprendre et maîtriser le système, ni d'appréhender pleinement l'environnement dans lequel celui-ci est déployé.

---

8. P. W. Singer, *Wired for War: The Robotics Revolution and Conflict in the 21st Century*, New York, Penguin, 2010, p. 9.
9. P. Scharre et K. Sayler, « Autonomous Weapons and Human Control », Center for a New American Security, avril 2016.

L'expérience israélienne est, de ce point de vue, édifiante. Comme l'explique Meron Rapoport, rédacteur en chef du magazine en ligne israélien *Local Call* – qui a travaillé avec *+972* dans ses enquêtes sur le recours à l'IA par Tsahal –, « la partie vérification humaine, qui doit s'assurer que la personne visée est bien la bonne, a été réduite au minimum, pas plus de vingt secondes dans certains cas, si bien que les soldats chargés de cette vérification ont le sentiment de simplement devoir entériner le choix de la machine ».

À cet enjeu de la vitesse s'ajoute un biais bien connu des algorithmes, l'effet « boîte noire », qui renvoie au fait que les techniques d'IA aboutissent parfois à des résultats que les programmeurs ne sont pas en mesure d'expliquer. De plus, si les opérateurs savent quels types de données ont été utilisés par l'algorithme pour formuler une recommandation – images satellite ou de drone, écoutes téléphoniques, renseignement d'origine électromagnétique, etc. –, ils n'ont pas connaissance de ce que contiennent précisément ces données. Sans pleine compréhension de la situation, l'humain a-t-il réellement la possibilité d'exercer son discernement ?

L'humain a-t-il réellement la possibilité d'exercer son discernement ?

Cette incompréhension s'accompagne en outre d'un biais d'automatisation, qui désigne la confiance démesurée que les opérateurs tendent à placer dans la machine. Parce qu'ils ne saisissent pas son raisonnement et qu'ils partent du principe qu'il effectue des calculs beaucoup plus sophistiqués qu'eux, les personnels militaires se contentent la plupart du temps d'approuver les choix du système.

Les craintes sur l'interaction entre l'humain et la machine existent depuis le XIX^e^ siècle. En 1956, dans son ouvrage *L'Obsolescence de l'homme : sur l'âme à l'époque de la deuxième révolution industrielle*, le philosophe Günther Anders proposait ainsi le concept de « décalage prométhéen ». Tel le Titan de la mythologie grecque condamné à un supplice éternel après avoir dérobé le feu sacré de l'Olympe pour en faire don aux hommes, expliquait Anders, l'homme moderne a repoussé les limites de la nature par la technique. Celle-ci finit toutefois par le dépasser : il en perd le contrôle. Le décalage prométhéen décrit alors l'écart entre les prouesses permises par la technique et les capacités limitées de l'homme – en particulier en ce qui concerne le sens de la mesure et la responsabilité.

Désormais, disait encore Anders, nous ne sommes plus capables que d'envisager les risques d'un phénomène particulier et de prendre de minces précautions pour les prévenir. Il nous est, en revanche, impossible

de considérer le phénomène technicien dans son ensemble. La technique impose dès lors ses critères, au premier rang desquels l'efficacité, et remplace toutes les autres valeurs. Du fait de sa complexité, elle devient littéralement incompréhensible : elle « dépasse l'entendement ».

Si le philosophe américain a développé ce concept pour penser l'arme nucléaire, celui-ci s'applique aujourd'hui remarquablement aux questions posées par le recours à l'IA dans les conflits. En effet, les techniques d'IA rendent plausible une forme de « guerre sans conscience », dans un phénomène de distanciation toujours accrue.

Maîtriser les armements intelligents

Tant Israël que l'Ukraine développent le discours d'une guerre existentielle face à leurs adversaires. Cette lutte pour la survie les autorise à faire sauter un certain nombre de préventions éthiques, comme en attestent les usages problématiques de l'IA observés sur les champs de bataille contemporains. Force est toutefois de constater que les emplois actuels constituent autant de précédents qui pourraient ouvrir la voie à des pratiques encore plus dangereuses, susceptibles d'être mises en œuvre par des acteurs malveillants, étatiques ou non étatiques. Il est donc indispensable de réfléchir à la maîtrise de ces nouveaux armements.

L'arsenalisation de l'IA suscite déjà de nombreuses préoccupations d'ordres éthique et juridique. En novembre 2018, à l'occasion du premier Forum de Paris sur la paix, le secrétaire général de l'Organisation des Nations unies António Guterres avait ainsi appelé à ce que soient « interdites par la législation internationale ces armes politiquement inacceptables et moralement révoltantes ». Des doutes existent en effet sur la capacité des techniques d'IA à se conformer au droit de la guerre ainsi que sur leur compatibilité avec le droit à la vie et le respect de la dignité humaine. Leurs opposants craignent par ailleurs qu'elles n'abaissent le seuil d'entrée en conflit, qu'elles ne donnent lieu à des escalades destructrices et qu'il soit impossible de déterminer les responsabilités en cas de crime de guerre.

C'est la raison pour laquelle la question du contrôle à exercer sur les armes fonctionnant grâce à l'IA fait désormais l'objet de discussions dans des enceintes multilatérales. À l'échelle internationale, le débat sur la régulation des armes autonomes a été engagé par des organisations non gouvernementales coalisées en une *Campaign to Stop Killer Robots* en 2012. La question a ensuite été discutée au Conseil des droits de l'homme puis dans le cadre de la Convention sur certaines armes classiques où, en 2016,

a été décidée la création d'un groupe d'experts gouvernementaux doté d'un mandat de discussion sur la question.

La place de l'humain dans le processus conduisant à l'emploi de la force létale par les armes autonomes est au centre des discussions de ce groupe d'experts gouvernementaux. Comme le signifie Noel Sharkey, roboticien et pionnier du mouvement *Stop Killer Robots*, « la vraie question est de savoir quel niveau de contrôle nous, humains, sommes prêts à concéder aux machines[10] ». À cet égard, l'expérience opérationnelle de l'IA militarisée, tant en Ukraine qu'à Gaza, tend à montrer que le fait de conserver un humain « dans la boucle » ne suffit pas à garantir un contrôle significatif sur les systèmes d'armes.

* * *

Dans le débat sur les conséquences morales du perfectionnement technique des systèmes d'armes, deux positions s'affrontent traditionnellement. D'un côté, la technique est pensée comme neutre : elle n'est qu'un moyen plus efficace d'accomplir une même mission. Pour détruire un char, que l'on utilise une mine antichar ou un essaim de drones ne fait aucune différence sur le plan moral. D'un autre côté, la technique est dite performative. La technologie affecte le contenu même des missions assignées aux militaires, en étendant largement le champ des opérations.

Au regard des guerres en Ukraine et à Gaza, l'IA, loin de contribuer à une guerre plus « propre » et respectueuse du droit international, inaugure une utilisation beaucoup plus massive et rapide de la force. Pour le dire crûment, elle permet de cibler plus de personnes, plus vite, à moindres frais et avec l'apparence d'une justification rationnelle. Il est donc urgent de réguler son utilisation.

PE

Mots clés
Intelligence artificielle
Guerre d'Ukraine
Guerre de Gaza
Innovation militaire

10. L. Belot, « Noel Sharkey : "Lorsque des machines répondront à des algorithmes secrets, personne ne pourra prédire l'issue d'un conflit" », *Le Monde*, 22 juillet 2015.

politique étrangère

Abonnez-vous !

Découvrez nos nouvelles offres d'abonnement sur le site www.revues.armand-colin.com

- Bénéficiez de services exclusifs sur le portail de notre diffuseur
- Accédez gratuitement à l'ensemble des articles parus depuis 2007
- Choisissez la formule papier+numérique ou e-only

TARIFS 2024

▶ *S'abonner à la revue*		France TTC	Étranger HT*
Particuliers	papier + numérique	☐ 85,00 €	☐ 105,00 €
	e-only	☐ 70,00 €	☐ 85,00 €
Institutions	papier + numérique	☐ 185,00 €	☐ 205,00 €
	e-only	☐ 140,00 €	☐ 160,00 €
Étudiants**	papier + numérique	☐ 70,00 €	☐ 75,00 €
	e-only	☐ 50,00 €	☐ 55,00 €

* Pour bénéficier du tarif **Étranger HT** et être exonéré de la TVA à 2,1 %, merci de nous fournir un numéro intra-communautaire
** Tarif exclusivement réservé aux étudiants sur présentation d'un justificatif

▶ *Acheter un numéro de la revue*	Tarif	**Numéro** (format X-20XX)	Quantité
Numéro récent (à partir de 2014)	☐ 23,00 €	.....	.....
Numéro antérieur à 2014	☐ 20,00 €	.....	.....

TOTAL DE VOTRE COMMANDE		..... €
FRAIS DE PORT (achat au n° seulement)	**3,00 €** pour une commande < à 35 € **0,01 €** pour une commande > à 35 €	..... €
TOTAL DE MA COMMANDE (commande + frais de port)		..... €

Bon de commande à retourner à :

DUNOD ÉDITEUR - Service Clients - 11, rue Paul Bert - CS 30024 - 92247 Malakoff cedex, France
Tél. 0 820 800 500 - Fax. 01 41 23 67 35 - Étranger +33 (0)1 41 23 66 00 - **revues@armand-colin.com**

Adresse de livraison

Raison sociale : .....
Nom : .....Prénom : .....
Adresse : .....
Code postal : |_|_|_|_|_| Ville : .....Pays : .....
Courriel : .....@.....

Règlement à l'ordre de Dunod Éditeur

☐ **Par chèque** à la commande
☐ **À réception de facture** (institutions uniquement)
☐ **Par mandat administratif** (institutions uniquement)

Date : _ _ /_ _ /_ _ _ _

Signature (obligatoire)

Je souhaite effectuer mes démarches en ligne ou par courriel/téléphone

- Je me connecte au site **www.revues.armand-colin.com**, onglet « ÉCO & SC. POLITIQUE »
- Je contacte le service clients à l'adresse **revues@armand-colin.com** ou au **0 820 800 500**

ifri 1979

ARMAND COLIN