

L'avantage de l'Ukraine : Comment l'IA modifie les rapports de force dans la guerre

Anselm Küsters et Jörg Köpke



© shutterstock

Une question de vie ou de mort : les technologies numériques comme l'intelligence artificielle (IA) marquent de plus en plus les événements sur le champ de bataille. Avec l'invasion de l'Ukraine par la Russie, la conduite de la guerre a été révolutionnée. Le front entre la Crimée et le Donbass devient tragiquement un terrain d'expérimentation. Mais malgré tous les succès de l'Ukraine et une supériorité de l'Occident, les expériences faites jusqu'à présent et les expériences d'IA montrent que les systèmes militaires autonomes ne sont durablement pas des armes miraculeuses.

Table des matières

1	Introduction.....	3
2	La puissance militaire à l'ère de l'IA	3
3	Vers une IA responsable ?.....	5
4	Tirer les leçons du passé.....	6
5	Risque : inconnu et non contrôlable.....	7
6	Une approche basée sur les risques avec des tests structurés	7

1 Introduction

Alors que les parlements et les gouvernements occidentaux discutent encore d'éventuelles exportations d'armes, les technologies numériques jouent depuis longtemps un **rôle militaire et géopolitique décisif**. L'invasion de l'Ukraine par la Russie est la première guerre dans laquelle les deux parties utilisent à grande échelle des moyens de combat numériques comme les drones.¹ À cela s'ajoutent près de 200 cyber-attaques quotidiennes, que Moscou utilise notamment dans le cadre de sa **guerre hybride**.² L'Ukraine tient tête à la Russie, puissance militaire mondiale, avec un succès étonnant grâce à l'utilisation créative de technologies à l'origine non militaires.³ Les satellites Starlink d'Elon Musk ou les drones volants de DJI en sont des exemples parlants. Le ministre ukrainien de la Transformation numérique, Mykhailo Fedorov, a récemment annoncé de nouveaux plans pour des systèmes autonomes modernes et des start-ups militaires.⁴

La guerre en Ukraine met en lumière le **rôle futur de l'IA dans le domaine militaire, compte tenu de** la menace d'un conflit à Taiwan poussé par la Chine. Pékin et Washington sont en train de développer des essais de drones autonomes qui communiquent entre eux. La Chine veut devenir cette année la première puissance mondiale en matière d'IA et a adopté une stratégie militaire agressive et axée sur l'innovation.⁵ La Grande-Bretagne mène également des recherches sur des robots pilotés par l'IA, qui doivent permettre aux troupes au sol de détruire des ponts d'importance stratégique - également motivées par l'expérience en Ukraine.⁶

Comment l'Europe occidentale doit-elle se positionner dans cette **compétition numérique** ? Des voix critiques demandent que l'IA militaire soit proscrite de manière générale au niveau international. D'autres considèrent que de tels systèmes sont indispensables pour ne pas mettre en jeu unilatéralement la sécurité de l'Occident. Les analyses du conflit ukrainien, les expériences faites avec les systèmes d'armes autonomes ainsi que les expérimentations sur les applications de l'IA montrent à quel point il est nécessaire d'évaluer systématiquement l'interaction entre l'homme et la machine afin d'éviter les effets négatifs, par exemple ceux d'un "tir ami". Les futures négociations sur la réglementation de l'IA dite responsable dans le domaine militaire devraient fixer des normes contraignantes en la matière.

2 La puissance militaire à l'ère de l'IA

L'automatisation des innovations technologiques militaires a progressé de manière croissante au cours des dernières années. Selon l'expert en défense Paul Scharre, à l'ère de l'IA, **quatre éléments clés sont décisifs pour la puissance militaire** : les données à collecter et à évaluer, un contrôle sans faille des chaînes d'approvisionnement en puces, le capital humain et la capacité d'innovation industrielle ainsi que l'intégration de l'IA dans l'économie, la société et l'armée. Scharre cite des exemples dans lesquels des agents dits d'IA simulent certaines situations de guerre.⁷

¹ [The Ukraine-Russia Drone War Is Crowdsourced and Made in China \(foreignpolicy.com\)](https://www.foreignpolicy.com/story/the-ukraine-russia-drone-war-is-crowdsourced-and-made-in-china).

² [La schizophrénie numérique - Le Quotidien Background](https://www.lequotidien.com/fr/actualites/technologie/la-schizophrénie-numérique).

³ Le drone tactique militaire TB2 Bayraktar d'un fournisseur turc était tout aussi pertinent dans les premiers temps. [TB2 Bayraktar : Grande stratégie d'un petit drone | IFRI - Institut français des relations internationales](https://www.ifri.fr/fr/actualites/le-dronage-tactique-tb2-bayraktar).

⁴ [L'Ukraine veut une armée de robots \(wired.com\)](https://www.wired.com/story/ukraine-robot-army).

⁵ [La force de soutien stratégique de l'APL et l'innovation en matière d'IA \(brookings.edu\)](https://www.brookings.edu/research/ai-innovation-and-strategic-support-for-ukraine/).

⁶ [L'armée britannique recherche des robots dotés d'IA pour permettre aux troupes de démolir des ponts au combat \(inews.co.uk\)](https://www.inews.co.uk/ukraine/british-army-research-robot-ai-combat/).

⁷ [Four Battlegrounds | Paul Scharre | W. W. Norton & Company \(wwnorton.com\)](https://www.wwnorton.com/insights/four-battlegrounds).

L'ère de l'IA va **redistribuer le pouvoir militaire**. La Russie semble actuellement avoir les plus mauvaises cartes en main. Depuis le début de la guerre, plus de **100 000 spécialistes en informatique**, soit 10 % de tous ceux qui travaillaient auparavant dans le secteur technologique, ont quitté la Russie.⁸ Dans le même temps, le nombre de start-ups militaires ukrainiennes a été multiplié par dix.⁹ En outre, la scène tech ukrainienne est mieux connectée au niveau international. Elle profite d'initiatives telles que "Army of Drones" pour obtenir plus rapidement du matériel de drone étranger. Le collectif international de hackers Anonymous parvient régulièrement à faire passer des critiques sur la guerre dans les médias russes et à publier des téraoctets de **fichiers piratés**.¹⁰ Enfin, les hackers ukrainiens de la "Cyber Resistance" ont pu s'emparer des courriels d'un espion russe qui avait voulu manipuler les élections présidentielles américaines de 2016.¹¹

Les conséquences de ce déséquilibre technologique sont déjà clairement visibles sur le champ de bataille. Kiev utilise l'IA plus efficacement que Moscou. Il s'agit notamment de **reconnaissance géographique et d'identification des cibles**. Par exemple, les données open source telles que les photos géopolitiques sensibles dans les médias sociaux sont analysées par l'IA.¹² Des développeurs ukrainiens ont entraîné des systèmes d'IA à identifier des chars ennemis camouflés à l'aide d'images en direct prises par des drones et à les détruire quasiment en temps réel.¹³ Les systèmes sont programmés pour apprendre en permanence de manière autonome. Comme ces drones n'utilisent pas de GPS en vol, les contre-mesures russes sont souvent restées vaines dans un premier temps. En réaction aux attaques de missiles russes depuis des navires de guerre en mer Noire, l'Ukraine a développé des bateaux-drones transportant des explosifs et utilisant l'IA pour reconnaître les cibles.¹⁴ L'entreprise ukrainienne de technologie Primer a adapté son service d'IA **pour la transcription** et la traduction de **la parole** afin de traiter rapidement les communications russes interceptées et d'extraire automatiquement des informations sur les forces armées.¹⁵ L'Ukraine profite du fait que les soldats russes communiquent souvent entre eux sans cryptage. Fin février, Fedorov a écrit que l'utilisation de technologies militaires innovantes était l'un des domaines dans lesquels l'Ukraine avait toujours une longueur d'avance sur la Russie.¹⁶

La Russie tente également d'utiliser des techniques numériques modernes. Mais **jusqu'à présent**, celles-ci se sont surtout limitées à **des attaques hybrides dans le cyberspace**.¹⁷ Les "Vulkan Files" récemment publiés montrent comment les services secrets russes orchestrent des cyberattaques, diffusent de la désinformation et censurent Internet avec l'aide de l'entreprise d'armement NTC Vulkan basée à Moscou.¹⁸ Sur le champ de bataille en revanche, le Kremlin a du mal à s'en sortir et a recours à des drones "kamikazes" d'Iran, relativement simples sur le plan technique. De nombreux indices

⁸ [Comment la Russie a tué son industrie technologique | MIT Technology Review](#).

⁹ [L'Ukraine veut une armée de robots \(wired.com\)](#).

¹⁰ [Les hackers dans la cyber-guerre : les attaques les plus curieuses d'Anonymous contre le Kremlin \(watson.de\)](#).

¹¹ [Piratage démocrate 2016 : des hackers ukrainiens affirment avoir piraté un espion russe - Golem.de](#).

¹² [Ukraine A Living Lab for AI Warfare \(nationaldefensemagazine.org\)](#).

¹³ [L'intelligence artificielle aide les drones à détruire les véhicules russes camouflés \(gagadget.com\)](#).

¹⁴ [L'Ukraine veut une armée de robots \(wired.com\)](#).

¹⁵ [Un an après : 10 technologies utilisées pendant la guerre en Ukraine - TechInformed](#).

¹⁶ [L'innovation technologique permet à l'Ukraine d'égaliser les chances face à la puissance militaire de la Russie - Atlantic Council](#)

¹⁷ Depuis octobre 2021 déjà, des pirates informatiques proches du FSB ciblent les comptes d'organisations ukrainiennes, et en janvier 2022, les experts de Microsoft ont identifié une opération de malware de grande envergure. [ACTINIUM targets Ukrainian organizations - Microsoft Security Blog](#) ; [Destructive malware targeting Ukrainian organizations - Microsoft Security Blog](#).

¹⁸ [La stratégie de cyberguerre de la Russie dévoilée - EURACTIV.fr](#).

montrent que lors de l'invasion de l'Ukraine, l'armée russe s'est principalement concentrée sur la guerre traditionnelle avec des chars, de l'artillerie et l'aviation. Selon Alex Karp, chef de l'entreprise de big data Palantir, la Russie est "massivement désavantagée" en raison du manque de technologies d'IA utilisées.¹⁹ Même les cyber-opérations techniquement réussies de Moscou n'ont pas abouti à des avantages opérationnels. L'attaque lancée au début de la guerre contre le fournisseur d'accès Viasat a certes paralysé les communications par satellite au-dessus de l'Ukraine, **mais elle n'a clairement pas réussi** à entraver les opérations de commandement et de reconnaissance ukrainiennes.²⁰ Au lieu de cela, elle a provoqué des effets de débordement involontaires en désactivant les modems satellites des éoliennes allemandes.

Le désavantage de la Russie en matière d'IA s'explique avant tout par une importante **différence de système**. Les secteurs technologiques des deux pays dépendent de leur **système d'ordre respectif**. En Russie, les entreprises d'État développent des équipements militaires pour le compte du gouvernement, tandis qu'en Ukraine, il existe un large éventail privé d'entreprises, de start-ups et d'inventeurs.²¹ L'arsenal ukrainien est plus diversifié et donc plus difficile à combattre. Selon Fedorov, l'Ukraine dispose du talent informatique et de la flexibilité nécessaires pour transférer en peu de temps de nouveaux concepts techniques "de la planche à dessin au champ de bataille".²² En fort contraste, les récentes activités d'espionnage des services de renseignement russes reposent également sur de nombreux éléments anciens, déjà connus lors de campagnes précédentes.²³ Au fur et à mesure que le secteur technologique russe, réglementé et mis à l'écart par Poutine, prend du retard, la capacité du Kremlin à utiliser l'IA militaire moderne diminue.

3 Vers une IA responsable ?

Même si les technologies numériques offrent des avantages à l'Occident en matière de politique militaire, elles soulèvent la question de leur maîtrise. Concrètement, l'utilisation accrue de fonctions autonomes et de systèmes d'IA dans la guerre en Ukraine pourrait **accélérer le développement d'armes totalement autonomes**, dont l'utilisation ne pourra jamais être totalement contrôlée. Au cours de la dernière décennie, des initiatives telles que la "Campaign to Stop Killer Robots", créée en 2012, sont devenues populaires. Les technologies potentiellement incontrôlables devraient être interdites à un stade précoce, car les activistes estiment qu'elles violent les droits de l'homme et conduisent ainsi à une augmentation des conflits.

La guerre d'agression menée par la Russie a toutefois donné une nouvelle dimension à ce débat. Dans le cadre du premier sommet mondial sur **l'IA responsable** dans le domaine militaire, qui s'est tenu aux Pays-Bas à la mi-février 2023, le département d'État américain a présenté une "déclaration politique" sur les conditions dans lesquelles de telles armes devraient être développées.²⁴ Cette déclaration ne

¹⁹ [Palantir CEO Alex Karp on Responsible AI in Warfare | REAIM 2023 - YouTube.](#)

²⁰ [Cyber Operations in Russia's War against Ukraine - Fondation Science et Politique \(swp-berlin.org\).](#)

²¹ [Des développeurs ukrainiens utilisent l'intelligence artificielle pour des bombardements par drones plus précis - Mezha.Media.](#) Il ne fait toutefois aucun doute que l'ordre économique ukrainien doit être réformé davantage. Même si la loi martiale subordonne actuellement l'ensemble de l'économie et de son administration aux exigences militaires et de sécurité, des déficits existaient déjà avant la guerre, notamment sous la forme de corruption, par exemple dans les domaines de la justice et des entreprises publiques. Pour une analyse, voir : [Reforming the Ukrainian Economy and State : The Unfinished Business | Publications | CESifo.](#)

²² [Le ministre ukrainien du millénaire mène la bataille numérique contre la Russie | The Hill.](#)

²³ [Campagne d'espionnage liée aux services de renseignement russes - Baza wiedzy - Portal Gov.pl \(www.gov.pl\).](#)

²⁴ [Déclaration politique sur l'utilisation militaire responsable de l'intelligence et de l'autonomie artificielles, ministère de l'État.](#) Pour une analyse, voir : [The US Pushing for Responsible AI in Military Use \(holisticai.com\).](#)

prévoit pas d'interdiction de l'IA militaire, mais dresse une liste abstraite des "meilleures pratiques". Elle stipule ainsi que les armes IA ne devraient être développées qu'en accord avec les lois internationales, et que les principes techniques devraient être transparents. Certains chercheurs ont en outre réfléchi à la manière de concevoir des systèmes militaires autonomes de manière à ce qu'ils se comportent au moins mieux que les soldats conventionnels sur le plan éthique.²⁵

Dans la situation géopolitique actuelle, une exigence d'interdiction basée sur des principes éthiques n'est toutefois plus communicable, elle serait même **naïve** du point de vue occidental. La guerre en Ukraine montre, en tant que **laboratoire d'essai** quasi **tragique**, que l'IA sera utilisée dans les conflits futurs, en dépit de tous les principes éthiques. Les avantages sur le champ de bataille sont trop séduisants : pouvoir analyser de grandes quantités de données, prédire les mouvements de l'ennemi et réagir rapidement à d'éventuelles menaces. Mais les armes IA autonomes peuvent également entraîner des problèmes incontrôlables dans le propre camp, comme les "tirs amis". C'est pourquoi il est important, non seulement du point de vue éthique mais aussi du point de vue de la stratégie militaire, de développer à temps **des stratégies pour leur surveillance** qui tiennent compte des erreurs antérieures des systèmes autonomes.²⁶

4 Tirer les leçons du passé

L'expérience acquise jusqu'à présent avec les systèmes militaires automatisés révèle de graves problèmes qui augmenteront de manière exponentielle à l'ère de l'IA. Pendant la guerre en Irak, par exemple, un Tornado britannique a été abattu par la marine américaine. Un programme informatique américain avait **classé à tort** l'avion de combat **comme un missile irakien**. Les critères programmés dans le système de défense antiaérienne Patriot auraient dû être beaucoup plus restrictifs compte tenu des capacités de l'Irak à l'époque, comme l'a révélé plus tard une enquête parlementaire.²⁷

Cet incident est répertorié dans la **AI Incident Database**, une encyclopédie en ligne répertoriant les incidents d'IA connus, sous la rubrique "erreurs lourdes de conséquences".²⁸ La base de données contient de nombreux autres cas dans lesquels des systèmes d'armes automatiques ont fait des victimes involontaires en raison de classifications erronées.²⁹ Les experts doutent qu'une arme autonome soit un jour en mesure de faire une distinction adéquate entre les cibles civiles et militaires.³⁰ De tels systèmes enfreignent donc ce que l'on appelle le **principe de discrimination**, selon lequel une distinction doit être faite entre les militaires et les civils lors de l'utilisation de la force.³¹

Les problèmes de classification décrits pourraient s'intensifier avec la prochaine génération d'IA militaire, comme les essaims de drones automatisés. Ainsi, les systèmes d'armes basés sur l'IA ont besoin de données complètes, pertinentes et granulaires pour être entraînés. Cependant, la **nature dyna-**

²⁵ Arkin, R. (2009). *Governing Lethal Behavior in Autonomous Robots* (1st ed.). Chapman and Hall/CRC.

²⁶ [Comprendre les erreurs introduites par les applications militaires AI \(brookings.edu\)](#).

²⁷ [maaszg710.doc \(publishing.service.gov.uk\)](#).

²⁸ Atherton, Daniel. (2003-03-22) Incident Number 444. in Lam, K. (ed.) *Artificial Intelligence Incident Database*. Responsible AI Collaborative. Retrieved on March 1, 2023 from [incidentdatabase.ai/cite/444](#).

²⁹ Atherton, Daniel. (2003-04-02) Incident Number 445. in Lam, K. (ed.) *Artificial Intelligence Incident Database*. Responsible AI Collaborative. Retrieved on March 1, 2023 from [incidentdatabase.ai/cite/445](#).

³⁰ Kallenborn, Z. (2021). Rencontre avec l'arme du futur de la destruction massive, le Drone Swarm. *Bulletin des scientifiques atomiques*, <https://thebulletin.org/2021/04/meet-the-future-weapon-of-mass-destruction-the-drone-swarm/>.

³¹ Dresp-Langley Birgitta (2023), The weaponization of artificial intelligence : What the public needs to be aware of, *Frontiers in Artificial Intelligence* 6, <https://www.frontiersin.org/articles/10.3389/frai.2023.1154184>.

mique, complexe et hostile des environnements de conflit rend leur application en dehors des laboratoires extrêmement sujette aux erreurs, car les facteurs nouveaux ou imprévisibles ne sont pas inclus dans les données d'entraînement.³² Cela change maintenant : chaque jour que dure le conflit ukrainien, les systèmes d'IA sont entraînés avec des données réelles provenant d'un champ de bataille réel.³³ Il est donc **plus intéressant** pour des pays comme la Chine, qui nourrit ses propres ambitions pour les systèmes d'IA militaires, **de fournir des armes afin de profiter des données**.

5 Risque : inconnu et non contrôlable

Compte tenu de ces problèmes, il existe actuellement un consensus prédominant sur le fait que les systèmes d'IA militaires devraient offrir une combinaison de processus automatisés et de possibilités d'intervention humaine. Même si la compréhension d'un tel modèle "**human in the loop**" est en principe à saluer, il faut se garder de croire à tort, au vu des décisions de vie ou de mort lourdes de conséquences prises par les systèmes d'armes, qu'une telle combinaison d'hommes et de machines est suffisante pour une utilisation sûre et robuste. En effet, les humains acceptent souvent la décision recommandée d'un système d'IA, même si elle est erronée - un problème appelé **surréalisme de l'IA**, ou "confiance aveugle" en l'IA.

L'interaction entre l'homme et la machine est donc difficile à évaluer, car les hommes ne réagissent pas toujours de manière rationnelle aux recommandations d'un ordinateur.³⁴ Ainsi, lors d'une expérience, des participants ont suivi les conseils délibérément mal programmés de l'algorithme, même lorsqu'ils auraient dû mieux savoir depuis longtemps.³⁵ Certains chercheurs espèrent réduire la confiance aveugle dans les systèmes d'IA en les obligeant à **expliquer leurs décisions**. Mais selon les tests, de telles explications ne font qu'augmenter la probabilité que les gens acceptent la recommandation de l'IA - indépendamment du fait qu'elle soit correcte ou non.³⁶

Une solution qui fonctionne, du moins expérimentalement, consiste non seulement à fournir une explication, mais aussi à encourager les gens à s'y confronter cognitivement.³⁷ On peut toutefois se demander s'il reste suffisamment de temps pour un processus aussi sophistiqué lorsque des millisecondes sont en jeu sur le champ de bataille. L'IA militaire traite de tâches complexes, ce qui implique que les explications de l'IA seront souvent aussi complexes à comprendre que la tâche elle-même. Un expert qui s'est penché sur les incidents de "tirs amis" évoqués en Irak prévient que les détails de l'utilisation de missiles balistiques sont "**trop complexes et trop limités dans le temps** pour une implication humaine directe".³⁸

6 Une approche basée sur les risques avec des tests structurés

³² Michel Hollande, Arthur. 2021. Known Unknowns : Data Issues and Military Autonomous Systems. Genève : Institut des Nations Unies pour la recherche sur le désarmement. <https://doi.org/10.37559/SecTec/21/A11>.

³³ [Ukraine A Living Lab for AI Warfare \(nationaldefensemagazine.org\)](https://www.nationaldefensemagazine.org/articles/story/ukraine-a-living-lab-for-ai-warfare).

³⁴ [Algorithmic Risk Assessment in the Hands of Humans \(iza.org\)](https://www.iza.org/publications/papers/10000).

³⁵ Biermann, Jan et Horton, John J. et Walter, Johannes, Algorithmic Advice as a Credence Good (2022). ZEW - Centre for European Economic Research Discussion Paper No. 22-071, <http://dx.doi.org/10.2139/ssrn.4326911>.

³⁶ [\[2006.14779\] Le tout accomplit-il ses parties ? The Effect of AI Explanations on Complementary Team Performance \(arxiv.org\)](https://arxiv.org/abs/2006.14779).

³⁷ [\[2212.06823\] Des explications peuvent réduire la surréaction des systèmes d'IA lors de la prise de décision \(arxiv.org\)](https://arxiv.org/abs/2212.06823).

³⁸ [Patriot Wars | Center for a New American Security \(en-US\) \(cnas.org\)](https://www.cnas.org/en-us/patriot-wars).

Alors que l'IA devient de plus en plus pertinente dans le domaine militaire tout en étant sujette à des erreurs, le débat sur sa réglementation est à la traîne.³⁹ Il n'existe **pas d'accords multilatéraux**, de **processus de certification ou de normes mondiales** garantissant des systèmes d'armes IA robustes et fiables. Il est significatif que la déclaration américaine sur l'IA militaire responsable mentionnée plus haut ne soit pas juridiquement contraignante. Les négociations actuelles de l'ONU sur les systèmes d'armes autonomes létaux à Genève piétinent.⁴⁰ Pourtant, de telles règles s'imposent d'urgence, car selon un éminent informaticien, une conception éthique des armes IA est certes "théoriquement intéressante", mais "impraticable".⁴¹

L'inspiration pourrait venir de la **loi sur l'IA** que les législateurs européens sont en train de négocier. La proposition suit une **approche basée sur les risques** en interdisant les pratiques d'IA particulièrement nuisibles. Même si la proposition de loi actuelle de l'UE exclut explicitement les systèmes d'IA militaires, son cadre et ses exigences horizontales peuvent également contribuer au développement de normes pertinentes pour les applications d'IA dans le domaine militaire.⁴² On pourrait ainsi imaginer des catégorisations analogues selon lesquelles les armes autonomes létales seraient interdites, tandis que tous les autres systèmes d'IA militaires devraient satisfaire à des exigences en matière de gestion des risques, de documentation, de transparence, de vérifiabilité, de robustesse et de cybersécurité.

Étant donné que les humains échouent souvent dans le suivi des recommandations de l'IA, l'efficacité des modèles militaires "human-in-the-loop" doit être **évaluée de manière structurée**.⁴³ Une telle documentation transparente favoriserait un discours politique plus rationnel sur ce sujet, car les recherches menées jusqu'à présent sur les systèmes d'armes autonomes sont presque exclusivement appliquées de manière confidentielle dans le domaine militaire.⁴⁴ Si ces tests révèlent que les humains ne peuvent pas contrôler efficacement les soi-disant drones tueurs ou autres systèmes d'IA, ils devraient être inscrits dans la catégorie des IA militaires interdites.

L'attaque de la Russie contre l'Ukraine ainsi que les tensions géopolitiques croissantes avec la Chine obligent les politiques occidentaux à se pencher sérieusement sur l'utilisation de l'IA militaire. Mais les conséquences potentielles de l'utilisation d'armes pilotées par l'IA ne peuvent être que vaguement évaluées. C'est pourquoi l'opinion publique doit être **sensibilisée aux dangers**. La tâche de la politique est de fixer **des conditions cadres contraignantes** avec des catégorisations juridiques, des obligations de transparence et des tests structurés de la possibilité de surveillance humaine de ces systèmes.

³⁹ [Amazon.com : Death machines : The ethics of violent technologies : 9781526114846 : Schwarz, Elke : Livres.](#)

⁴⁰ [Négociations de la CCW à l'ONU ? - Background du Tagesspiegel.](#)

⁴¹ Michael Wooldridge, A Brief History of Artificial Intelligence, New York 2020, p. 195.

⁴² [Challenges of Governing AI for Military Purposes and Spill-Over Effects of the AI Act | Futurium \(europa.eu\).](#)

⁴³ Analogie pour d'autres domaines de l'IA : [The AI Act should use humans to monitor AI only when effective - EURACTIV.](#)

⁴⁴ Dresp-Langley Birgitta (2023), The weaponization of artificial intelligence : What the public needs to be aware of, Frontiers in Artificial Intelligence 6, <https://www.frontiersin.org/articles/10.3389/frai.2023.1154184>.



Auteur :

Dr. Anselm Küsters, chef du département Numérisation & Nouvelles technologies

kuesters@cep.eu

Dr. Jörg Köpke, directeur de la communication du Centre de politique européenne

koepke@cep.eu

Traduction :

Victor Warhem, représentant du cep Network en France.

warhem@cep.eu

Centre de politique européenne FREIBURG | BERLIN

Kaiser-Joseph-Straße 266 | D-79098 Fribourg

Schiffbauerdamm 40 Pièces 4205/06 | D-10117 Berlin

Tél. + 49 761 38693-0

Le **Centrum für Europäische Politik** FREIBURG | BERLIN, le **Centre de Politique Européenne** PARIS, et le **Centro Politiche Europee** ROMA forment le **Centres for European Policy Network** FREIBURG | BERLIN | PARIS | ROMA.

Le Centre de Politique Européenne, à but non lucratif, analyse et évalue la politique de l'Union européenne indépendamment des intérêts particuliers et des partis politiques, dans une orientation fondamentalement favorable à l'intégration et sur la base des principes réglementaires d'un ordre libéral et d'une économie de marché.