

## RESEARCH OUTPUTS / RÉSULTATS DE RECHERCHE

### L'intelligence artificielle

Lambert, Dominique; Ruffo De Bonneval De La Fare Des Comtes De Sinopoli De Calabre, Marie-Des-Neiges

*Published in:*  
DSI

*Publication date:*  
2019

*Document Version*  
le PDF de l'éditeur

#### [Link to publication](#)

*Citation for published version (HARVARD):*

Lambert, D & Ruffo De Bonneval De La Fare Des Comtes De Sinopoli De Calabre, M-D-N 2019, 'L'intelligence artificielle: nouveau défi pour l'éthique?', *DSI*, vol. Hors-Série, numéro 65, pp. 90-92.

#### **General rights**

Copyright and moral rights for the publications made accessible in the public portal are retained by the authors and/or other copyright owners and it is a condition of accessing publications that users recognise and abide by the legal requirements associated with these rights.

- Users may download and print one copy of any publication from the public portal for the purpose of private study or research.
- You may not further distribute the material or use it for any profit-making activity or commercial gain
- You may freely distribute the URL identifying the publication in the public portal ?

#### **Take down policy**

If you believe that this document breaches copyright please contact us providing details, and we will remove access to the work immediately and investigate your claim.



# L'INTELLIGENCE ARTIFICIELLE : UN NOUVEAU DÉFI POUR L'ETHIQUE ?

Le plus souvent, on considère que les objets technologiques sont neutres éthiquement et que les problèmes naissent de leur usage. Aussi, toute évaluation éthique ne saurait-elle être plus avancée que les projets d'Intelligence Artificielle (IA) actuellement en développement. La première partie de cet article dessinera néanmoins un tour d'horizon des logiciels existants non classifiés et de leurs usages possibles pour la défense, ainsi que les enjeux éthiques qu'ils induisent. Dans un deuxième temps, le professeur Lambert offrira une perspective générale sur l'éthique de l'IA et la nécessité de s'appuyer en parallèle sur une régulation juridique.

Certaines composantes militaires que l'on retrouve dans la vie civile peuvent être confiées à l'IA : le recrutement, la gestion de la logistique, ou même, pour la composante médicale, l'utilisation de logiciels d'aide au diagnostic pour évaluer la gravité de l'état des patients amenés en urgence et faciliter leur triage. La surveillance peut aussi être confiée à l'IA, il s'agit alors d'algorithmes de détection, comme ceux qui sont utilisés dans les aéroports. Mais une étude de l'université Queen Mary (Londres) affirmait en 2001 que ces systèmes n'étaient pas très efficaces pour les foules. Il serait dangereux de ne se fier qu'à ce type de systèmes, mais il ne serait pas absurde par exemple de s'en servir pour aider une section à sécuriser un *checkpoint*, repérer des tentatives

Dominique LAMBERT  
et Marie-des-Neiges RUFFO  
Université de Namur.

“ Si des systèmes de *deep learning* tels que les classificateurs peuvent diagnostiquer des mélanomes de la peau avec 7,5% d'erreurs, les dermatologues restent plus efficaces, avec 3,4%. Cependant, le diagnostic conjoint du logiciel et des dermatologues permet de réduire l'erreur à seulement 0,5%. ”

Photo ci-dessus :

Le drone tactique turc Bayraktar a d'emblée été conçu pour l'emport d'armement. La question d'une autonomie décisionnelle des drones dans un environnement déjà largement chaotique laisse bon nombre d'armées sceptiques. (© Ukroboronprom)

kamikazes, etc. Il serait en revanche plus risqué, pour les relations entre les militaires et les populations locales, de ne se fier qu'aux algorithmes, en supprimant le contact humain.

## QUESTIONS ÉTHIQUES

Le premier usage de l'IA spécifique à la défense qui soulève des questions éthiques est la décision du tir. Celle-ci peut être automatique, comme cela se produit avec une mine antipersonnel. Cet exemple indique que laisser un engin décider seul du déclenchement de la réponse létale est en soi problématique. L'utilisation de l'IA n'y changerait pas grand-chose, puisque des erreurs peuvent aussi se produire. L'abondance de techniques ne signifie rien en matière d'infailibilité. On se souvient, par exemple, que l'équipage du croiseur Vincennes n'avait pas osé mettre en doute, pour la décision de tir, l'efficacité présumée de la machine (1). Soyons donc plus que prudents avant de faire aveuglément confiance à l'IA pour classifier une cible : la méfiance doit être de rigueur. Si des systèmes de *deep learning* tels que les classificateurs peuvent diagnostiquer des mélanomes de la peau avec 7,5% d'erreurs, les dermatologues restent plus efficaces, avec 3,4%. Cependant, le diagnostic conjoint du logiciel et des dermatologues permet de réduire l'erreur à seulement 0,5% (2).

Le traitement d'informations pour le renseignement est le second usage éthiquement problématique de l'IA. Edward Snowden a révélé (3) que la NSA utilisait un algorithme d'apprentissage appelé Skynet (4). Utilisé au Pakistan, il se base sur les données téléphoniques, du type *big data*, pour déterminer qui est un terroriste et qui figurera sur la *black list* des raids de drones. En plus de l'aspect éthiquement problématique de faire désigner par une machine des cibles humaines et de fixer un seuil arbitraire pour la « cote » qui fera de vous un terroriste ou non, l'efficacité et la valeur scientifique de l'algorithme sont mis en question. Le directeur de l'Human Right Data Analysis Group, Patrick Ball, met en doute la valeur scientifique de l'algorithme et a décrit les méthodes de la NSA comme « *ridiculement optimistes* » et comme de « *complètes conneries* » (5). Les choix épistémologiques opérés pour établir les critères qui qualifient une vie de « terroriste » ne sont pas non plus à l'abri d'erreurs. Le risque de faux positifs est important : l'un des journalistes d'Al-Jazeera s'est vu listé comme membre d'Al-Qaïda parce qu'il interviewait des terroristes. Le plus inquiétant dans cette qualification erronée n'était pas l'erreur d'interprétation de la machine, mais bien plutôt qu'elle ait été présentée par un humain comme un succès. Le développement du traitement de l'information par l'IA se poursuivra néanmoins forcément puisque la DARPA a lancé, en janvier 2019, un appel à projets appelé KAIROS (Knowledge-directed

Artificial Intelligence Reasoning Over Schemas). L'avenir nous en dira plus.

Pour créer des algorithmes (6), il faut suivre un processus. Pour créer Skynet, il a fallu définir des objectifs, des stratégies pour les atteindre, récolter des données, les interpréter sous forme de statistiques, etc. Chacune de ces étapes est pertinente pour

“ La représentation (ou la « construction ») algorithmique d'une réalité pose des questions éthiques fondamentales si cette réalité est une personne humaine, et si elle n'est pas assortie d'une analyse critique des algorithmes et de leurs biais constitutifs. ”

une évaluation éthique. Savoir si les données récoltées sont justes, complètes, non biaisées, relève de l'éthique. Il en va de même pour la manière dont elles seront interprétées. Le statisticien connaît les conditions essentielles pour que les statistiques aient du sens (au minimum la taille de l'échantillon), les moyens de les truffer, leurs limites, tout

comme l'informaticien connaît les limites de l'*autonomie* ou de l'*intelligence* d'un système : ce dernier ne fait pas « n'importe quoi ». Ni l'un ni l'autre ne se laissent bluffer par le vocabulaire commun ou par l'apparente neutralité d'un chiffre. Mais qu'en est-il de ceux qui ne sont pas des experts ? S'ils n'ont que leurs fantasmes pour les guider, n'attendent-ils pas plus de la technique que ce qu'elle est en état de leur donner ? Ce seront les donneurs d'ordres, les politiciens, les hommes de terrain, qui risquent d'exiger des objectifs irréalistes, que l'on pourrait être tenté en retour d'atteindre par des stratégies non éthiques ; là est le danger.

Que ces usages éthiquement problématiques de l'IA nous disent-ils des problèmes éthiques fondamentaux sous-jacents ? Dans ce contexte technologique, toute réalité est réduite à une représentation algorithmique et numérique, qui n'en retient que certains aspects et en occulte ou en oublie d'autres, en fonction de certains biais ou choix dictés *a priori* par des humains ou par des systèmes capables de faire émerger, par *deep learning*, des « classes approximativement correctes » de décisions (7). Le problème éthique apparaît ici dès lors que l'on dissimule ces biais en raison d'intentions discutables ou qu'on les oublie par négligence.

La représentation (ou la « construction ») algorithmique d'une réalité pose des questions éthiques fondamentales si cette réalité est une personne humaine, et si elle n'est pas assortie d'une analyse critique des algorithmes et de leurs biais constitutifs. Si l'on doit juger une personne devant un tribunal, ou si l'on doit décider de prendre pour cible telle personne qui est identifiée comme un ennemi légitime, il est souvent difficile et parfois dangereux de se limiter à un ensemble de paramètres pouvant être traités algorithmiquement. En effet, de telles décisions demandent justement de prendre en compte la complexité des êtres et des situations. Une question éthique fondamentale est donc celle qui est suscitée par *la mutilation d'une réalité dont la richesse devrait être prise en compte dans certaines décisions cruciales*. La réponse à cette interrogation éthique devrait idéalement contribuer à fonder un cadre légal protégeant certains aspects de la vie des individus, et des groupes humains, contre les possibles effets néfastes de cette réduction de pans entiers de la vie à des langages formels.

L'opacité constitutive (non voulue, mais liée à des systèmes complexes) de systèmes qui effectuent le *deep learning* (au moyen de réseaux de neurones par exemple) et qui apprennent à identifier, par eux-mêmes, une menace peut constituer un deuxième problème éthique. En effet, une personne pourrait se retrouver identifiée et fichée



Le CIC de l'USS Vincennes. La destruction de l'Airbus d'Iran Air est plus due à une utilisation incomplète du système Aegis – sur lequel le nouvel équipage était insuffisamment entraîné – qu'à un excès de confiance en l'automatisation. (© US Navy)



Le robot d'appui LS3. Comme nombre de mules, l'engin est programmé pour suivre son équipe. (© US Marine Corps)

comme dangereuse, sur la base de l'utilisation d'une machine dont on ne comprendrait pas entièrement le fonctionnement et les critères d'identification qu'elle mobilise. La *non-transparence des programmes et des processus de classification* pose donc une question fondamentale.

### RESPONSABILITÉ DES AGENTS ET INTENTIONS DES AUTORITÉS LÉGITIMES

Les deux problèmes que nous venons de soulever, mutilation volontaire ou involontaire d'une situation complexe ou absence de transparence des processus d'acquisition d'informations et de décision renvoient à la question de la *responsabilité*. Une décision cruciale engageant la vie ou la mort d'une personne, son exclusion, sa manipulation, sa surveillance, etc., demande que soit identifié l'*agent* qui est à l'origine de cette décision. De plus, ce dernier doit être capable de répondre de ses actes, en explicitant les raisons qui l'ont poussé à agir de telle ou telle façon. Cette capacité à répondre d'actes dont on est la source est constitutive de la responsabilité juridique et éthique. L'opacité des processus et des critères décisionnels, voire des biais de programmation, peut servir à dissimuler les responsabilités et les responsables, ce qui constitue un problème majeur du point de vue légal et moral.

Une autre question éthique fondamentale posée par l'usage de l'IA est le *risque d'une perte du sens d'une action politique ou militaire* lors de la délégation de pouvoirs importants à une machine exerçant sur ceux qui l'utilisent une énorme fascination liée à ses performances (la vitesse des processus, la

puissance calculatoire, etc.). Dans ce cas de figure, les intentions et les contenus politiques ou militaires ne seraient plus déterminants ou au moins premiers. L'autorité se laisserait guider, en grande partie, par des suggestions produites par des programmes et des machines ayant, peu à peu, perdu le contact avec les *finalités profondes de l'action*, alors que le système d'IA ne devrait être qu'un outil au service de la décision et de ces finalités. Le risque est, ici, la dépolitisation des décisions et éventuellement l'absence de justification de l'intérêt militaire de certaines actions, ce qui est contraire au *jus in bello*.

“ *La non-transparence des programmes et des processus de classification pose donc une question fondamentale.* ”

Nous l'avons mentionné, l'utilisation de systèmes d'IA qui ont la capacité de surveiller des personnes ou des groupes, d'acquiescer sur eux des informations et de les mémoriser, de faire émerger, à leur propos, des profils standardisés mène à des décisions qui peuvent conditionner fortement leur vie. Pour éviter cet écueil, nous devons tenir compte de critères éthiques fondamentaux. Parmi ceux-ci nous voudrions souligner :

- le respect de la complexité des situations caractérisant les personnes humaines et la conscience des biais et des réductions inhérents à la construction de logiciels ; cela pour éviter le développement de procédures d'exclusion, de discrimination, de manipulation ou

d'autres actions nuisibles produites justement en raison de filtres réducteurs et de normalisation hâtive ;

- l'importance éthique du maintien effectif et de l'identification claire de la *responsabilité des agents* qui mettent en œuvre ces techniques d'IA ;

- le fait que tout usage de l'intelligence artificielle dans le domaine de la sécurité ou de la défense devrait toujours se faire en maintenant un lien clair et solide avec les *contenus des intentions des autorités légitimes*. La performance des systèmes est telle qu'un effet non négligeable de fascination pourrait conduire à oublier progressivement et insensiblement ces intentions et ces contenus, en plaçant les autorités à la remorque de décisions sans véritable justification profonde.

On voit que les problèmes éthiques majeurs ne sont pas liés, comme tels, à l'utilisation de l'IA (qui peut par ailleurs aider le décideur et lui faire éviter des catastrophes). Ils sont suscités par une utilisation de l'IA qui premièrement fait disparaître l'utilisateur comme *acteur responsable*, pleinement conscient de la finalité de ses actions et de ses décisions et deuxièmement *réduit* celui qui est l'objet de cette utilisation à un ensemble de données qui ne respecte en rien sa richesse et sa singularité.

L'étude approfondie de ces exigences éthiques pourrait, éventuellement, donner à penser pour une construction de normes juridiques tenant compte impérativement de ce lien fondamental au décideur humain responsable et du respect de celui qui est la cible de son action (8). Pour garantir l'éthique à venir, nous proposons une ligne rouge psychologique : ne jamais confondre l'avis d'un algorithme avec un ordre, et une ligne rouge stratégique : ne jamais laisser la décision politique et géopolitique à des logiciels, l'enjeu majeur étant de ne jamais abandonner son humanité et son jugement humain prudent ou *phronésis*. ■

#### Notes

- (1) Abattant ainsi le vol civil 655 d'Iran Air le 3 juillet 1988.
- (2) Tom Gruber « Comment l'IA peut améliorer notre mémoire, notre travail et notre vie sociale », TED Talks, 2017.
- (3) « La NSA a un programme d'espionnage appelé Skynet », *Libération*, 10 mai 2015.
- (4) Il n'est pas unique, on évoque aussi « MonsterMind ».
- (5) Christian Grothoff et J. M. Porup, « The NSA's SKYNET program may be killing thousands of innocent people », *Arstechnica.com*, 16 février 2016.
- (6) Selon la mathématicienne Cathy O'Neil, les algorithmes entrent dans la catégorie de ce que nous nommons intelligence artificielle.
- (7) Cf. L. Vaillant, *Probably Approximately Correct. Nature's Algorithms for Learning and Prospering in a Complex World*, Basic Books, New York, 2013.
- (8) Nous renvoyons ici à H. Jacquemin et M. Nihoul (dir.) *Vulnérabilité et droits dans l'environnement numérique*, Larcier, Bruxelles, 2018 et à H. Jacquemin et A. de Streef (dir.), *L'intelligence artificielle et le droit*, Larcier, Bruxelles, 2017.



DÉFENSE & SÉCURITÉ INTERNATIONALE

**HORS-SÉRIE**  
**65**

**L'IA EN SOUTIEN  
DU COMBAT  
AÉROTERRESTRE**

**L'IA AU SERVICE  
DES STRATÉGIES  
D'INFLUENCE MILITAIRES**

# INTELLIGENCE ARTIFICIELLE

## Vers une révolution militaire ?



ENSTA Bretagne

EBP82028  
1510645

- VERS LA PROLIFÉRATION DES IA MILITAIRES ?**
- QUELLE PLACE DANS LA ROBOTIQUE DE COMBAT ?**
- LES APPLICATIONS, DU RENSEIGNEMENT AU MCO**
- LES INDUSTRIELS SUR LES RANGS**
- TERRE, AIR, MER : QUELLES VISIONS ?**

En partenariat avec :  
**CENTRE DE RECHERCHE DES ÉCOLES  
DE SAINT-CYR COËTQUIDAN (CREC)**

L 17480 - 65 H - F: 10,95 € - RD



Retrouvez-nous sur [Areion24.news](http://Areion24.news)



Éditorial

03

## DÉFINITION ET PERSPECTIVES

**DÉFINITION ET EMPAN DE L'INTELLIGENCE ARTIFICIELLE**  
Jean-Gabriel GANASCIA

08

**INTELLIGENCE ARTIFICIELLE ET ROBOTS MILITAIRES**  
Patrick BEZOMBES

12

## POSSIBILITÉS D'APPLICATIONS MILITAIRES

**INTELLIGENCE ARTIFICIELLE : LE CHAMP DES POSSIBLES**  
Gérard de BOISBOISSEL

18

**VERS LA PROLIFÉRATION DES INTELLIGENCES ARTIFICIELLES MILITAIRES ?**  
Joseph HENROTIN

22

**FORCES ET FAIBLESSES/VULNÉRABILITÉS DE L'IA DANS UN AFFRONTÉMENT FUTUR**  
Thomas REYDELLET

26

**L'INTELLIGENCE ARTIFICIELLE COMME CATALYSEUR DU CYCLE DE LA DÉCISION EN OPÉRATIONS**  
Damien SAUGET

30

**LORSQUE L'INTELLIGENCE ARTIFICIELLE ÉLARGIT LE SPECTRE DES MENACES CYBER**  
Thierry BERTHIER

34

**L'INTELLIGENCE ARTIFICIELLE AU SERVICE DU COMBAT AÉROTERRESTRE**  
Marc ESPITALIER

38

**L'IA POUR CONNAÎTRE L'INCONNAISSABLE : EMBARQUEMENT IMMÉDIAT À BORD DE L'ALSACE**  
Camille GIRARD

42

**L'INTELLIGENCE ARTIFICIELLE DANS L'ARMÉE DE L'AIR**  
Étienne FAURY et David PAPPALARDO

46

**L'IA AU SERVICE DES STRATÉGIES D'INFLUENCE MILITAIRES**  
Romain MIELCAREK

52

## ASPECTS TECHNOLOGIQUES

**ENTRETIENS CROISÉS : QUELLES VISIONS DANS L'INDUSTRIE ?**  
Emmanuel BRESSON

58

**LES ASPECTS TECHNOLOGIQUES DE L'IA ET SON INTÉGRATION AU SEIN DES SYSTÈMES MILITAIRES. LE POTENTIEL DES RÉSEAUX BAYÉSIENS**  
Emmanuel KEITA

66

**SPÉCIFICATION ET QUALIFICATION DES SYSTÈMES À BASE D'INTELLIGENCE ARTIFICIELLE**  
Alexandre HERVIEU

70

**COMMENT SUPERVISER ET CONTRÔLER LES PROCESSUS D'INTELLIGENCE ARTIFICIELLE EMBARQUÉS DANS LES SYSTÈMES AUTONOMES**  
Arnault IOUALALEN

74

## LES ENJEUX LIÉS À L'IA

**LA PLACE DE L'APPRENTISSAGE PROFOND DANS LES INTERFACES HOMME-MACHINE DE DEMAIN**  
Jean-Christophe SARRAZIN, Stéphane HERBIN et Adrien CHAN-HON-TONG

80

**LES BIAIS COGNITIFS ET L'IA**  
Benoit LE BLANC

84

**LA RESPONSABILITÉ JURIDIQUE DU MILITAIRE FACE AUX ENJEUX DE L'INTELLIGENCE ARTIFICIELLE**  
Gilles GUIHEUX

87

**L'INTELLIGENCE ARTIFICIELLE : NOUVEAU DÉFI POUR L'ÉTHIQUE ?**  
Dominique LAMBERT et Marie-des-Neiges RUFFO

90

**LE SOLDAT ET LE CYGNE NOIR. INTELLIGENCE ARTIFICIELLE ET INTELLIGENCE TACTIQUE : CONVERGENCE ET DISCORDANCE**  
Gilles HABEREY

93

**L'INTELLIGENCE ARTIFICIELLE, SOCLE DE NOS CAPACITÉS**  
Charles BEAUDOUIN

96