UN ARTICLE UBCOM

EDITION AVRIL 2023

L'IA: UNE ARME DE CONFLITS

EN QUOI L'INTELLIGENCE ARTIFICIELLE INFLUENCE-T-ELLE LES STRATÉGIES D'ATTAQUE ET DE DÉFENSE MILITAIRES ?

L'INTELLIGENCE ARTIFICIELLE : SON INFLUENCE SUR LES STRATÉGIES MILITAIRES

Ponctué par de nombreux conflits, de basses comme de hautes intensités, notre monde est entré dans une ère nouvelle dans laquelle l'équilibre des puissances évolue et se cherche sans cesse. La société moderne doit absorber le développement de nouvelles technologies, modifiant les règles du jeu des conflits internationaux. Dans la deuxième moitié du XIXe siècle, notre société mue par l'air industrielle grâce aux technologies majeures comme l'électricité, la turbine à vapeur, la chimie organique ou encore le moteur à explosion. Dès lors, scientifiques, chercheurs, ingénieurs, universités et entreprises n'ont cessé d'in--nover et de produire des technologies de plus en plus sophistiqués. En 1971, la firme Intel commercialise le premier microprocesseur : « 4004 », ouvrant la voie de l'ère numérique que l'on connaît aujourd'hui. Bousculée par des innovations constantes durant 50 ans, le monde développe dans la conjoncture actuelle des technologies auxquelles les scientifiques ne pouvaient songer à la fin des trente glorieuses.

Ces innovations, à la fois physiques et numériques, sont aujourd'hui implantées partout sur le globe ou presque. Si les termes de blockchain, cloud computing, intelligence artificielle, métavers, objets connectés sont des termes aujourd'hui répandus, il est de nature à se demander si elles sont utiles ou si elles présentent de sérieuses menaces à l'équilibre de notre monde moderne. Au niveau militaire, l'ère « High Tech », accompagnée des risques cyber qui lui sont logiquement associés, se présente à double tranchant. On note qu'entre 2016 et 2020, les incidents de cybersécurité dans les conflits armés ont augmenté de 235 %.[1] Les nouvelles technologies actuelles se présentent-elles comme favorables à la défense contre les cyberattaques ou représentent-elles les alliées parfaites de frappes cyber plus précises et dévastatrices ?

IA : QUELLES INFLUENCES DANS LES GUERRES CONVENTIONNELLES ?

L'IA est un domaine de l'informatique qui vise à créer des machines capables de fonctionner de manière autonome et de réaliser des tâches qui nécessitent normalement l'intelligence humaine. L'IA implique le développement de programmes informatiques qui peuvent apprendre, raisonner, planifier, percevoir, communiquer et prendre des décisions de manière autonome. Le *Machine learning* (apprentissage automatique) quant à lui, est une sous-discipline de l'IA qui implique l'utilisation de techniques et d'algorithmes pour permettre à un ordinateur de s'entraîner sur des données et d'apprendre à exécuter des tâches spécifiques, comme la classification d'images ou la prédiction de valeurs numériques.

ALLIÉS DES OPÉRATIONS D'ATTAQUE MILITAIRE

L'utilisation de l'IA et du *Machine learning* sont des technologies d'une efficacité grandissante dans les stratégies d'attaque militaire, grâce à l'efficacité et la précision des opérations. Mieux encore, l'IA permet de gagner un temps considérable donnant l'avantage tactique au premier qui a la bonne réponse. Ces innovations technologiques témoignent d'une utilité remarquable quel que soit l'élément dans lequel une attaque s'opère : dans les airs, sur la Terre, aussi bien qu'en mer. Le Président russe, Vladimir Poutine afirmait dans son discours annuel devant la Douma que celui qui maitrisera l'IA sera le maitre du monde. Cette vision se confirmera par la lettre ouverte publier le 29 mars dernier dans laquelle on trouve des signataires inattendu comme Elon Musk invitant à instaurer un moratoire sur le développement de l'IA qui pourrait remettre en cause l'équilibre social du monde dans un délai terriblement court.

Dans un scénario d'attaque aérienne coordonnée, le ciblage précis des frappes aériennes peut être amélioré considérablement grâce à l'IA. Certains algorithmes incluant des technologies de *Machine learning* sont capables d'être entraînés à identifier et analyser des cibles spécifiques, grâce à des capteurs radars ou optiques afin de focaliser la visée sur la cible prédéfinie et d'accompagner le co-pilote de chasse dans le

[1] Étude de l'Institut international de recherche sur la paix de Stockholm, 2020

déclenchement de la frappe aérienne. C'est le cas du bombardier furtif américain B-2 Spirit et du chasseur-bombardier F-35 Lightning II par exemple, qui utilisent des systèmes de ciblage avancé nommés respectivement "Advanced Targeting System" (ATS) et "Electro-Optical Targeting System" (EOTS),[2] afin de collecter des données en temps réel sur les cibles ennemies et les environs. De surcroît, ces technologies peuvent être utilisées pendant la période pré-opérationnelle en contribuant à l'élaboration de la meilleure approche d'attaque. Notamment en établissant des altitudes et des planifications de changements de paramètres de vol, afin de permettre aux avions d'échapper aux radars et aux missiles air-sol par exemple. Le logiciel américain d'IA "ALPHA"[3]en est l'un des plus performants. Utilisant des algorithmes d'apprentissage automatique, ce logiciel est capable de simuler les mouvements de l'ennemi et de ses missiles air-sol afin de développer des tactiques de défense optimales pour les avions de chasse. Le logiciel a été testé avec succès dans des simulations de combats aériens et a montré des résultats prometteurs pour améliorer la survie des avions de chasse dans des situations de combats intenses.

Quelques pieds plus bas, l'IA est un allié dans l'optimisation de la logistique de la chaîne d'approvisionnement. En effet, capable d'optimiser les itinéraires de transport en fonction des risques, les stocks de matériaux, la gestion des entrepôts et d'autres aspects de la logistique militaire, l'IA peut s'avérer redoutable. Les algorithmes de *Machine learning* peuvent quant à eux être utilisés pour prédire les besoins futurs et pour planifier en conséquence les transferts d'armes et de munitions. Le système "Joint Logistics Over-the-Shore" (JLOTS) de l'armée américaine utilise l'IA pour optimiser la logistique de la chaîne d'approvisionnement militaire en temps de guerre en planifiant les itinéraires de transport, en évaluant les risques de sécurité et en identifiant les obstacles potentiels. Le système utilise également des algorithmes d'IA pour prévoir les demandes de fournitures et matériaux, en fonction des opérations militaires en cours et des prévisions de la situation sur le terrain. Le système JLOTS est utilisé en particulier dans les zones côtières où les ports et les infrastructures de transport sont limités.

Encore quelques mètres en dessous de la surface de la terre, l'IA peut constituer une arme de détection pointue pour les attaques navales. Elle peut être d'une utilité primordiale dans l'analyse des signaux acoustiques et l'identification des signatures des sous-marins ennemis. C'est le cas notamment du très performant système de sonar trempé "AN/AQS-22 Airborne Low Frequency Sonar (ALFS)"[4]développé par la société Lockheed Martin pour l'US Navy.

Sonar trempé "AN/AQS-22 Airborne Low Frequency Sonar (ALFS). Source : Military Periscope

Installé sur des hélicoptères de la marine américaine, ce système ALFS utilise notamment l'IA pour reconnaître, dans les données acoustiques transmises par les sous-marins, les signatures acoustiques spécifiques émises par les bâtiments ennemis, même dans des conditions difficiles, telles que des environnements bruyants ou des eaux agitées. Mais le rôle de l'IA sous la surface de la mer ne s'en tient pas qu'à cela. Elle est également utilisée dans la détection de motifs dans les images sonar qui indiquerait la présence de mines ou de défense sous-marine.

Par exemple, le dispositif canadien "Automatic Target Recognition" (ATR)[5]de la société Kraken Robotics est installé sur des drones sous-marins autonomes, tels que le KATFISH, et est utilisé pour la détection et la classification des mines et des systèmes autonomes anti-torpilles. En utilisant l'IA pour la détection de motifs dans les images sonar, le système ATR est capable de fournir des informations précises et en temps réel sur les objets détectés, ce qui permet aux forces militaires de prendre des décisions plus éclairées pour assurer la sécurité de leurs bâtiments et de leurs équipages.

2 Journal of Applied Remote Sensing, Vol. 11, Issue 1, Janvier 2017
3 "Beyond video games: New artificial intelligence beats tactical experts in combat simulation" - Université de Cincinnati, USA, Juin2017
4 "Navy asks Thales to build AN/AQS-22 dipping sonar aboard MH-60 anti-submarine warfare (ASW) helicopters" - Military aerospace, Avril 2021
5 "Towed Sonar Upgraded with Automatic Target Recognition Software" - Unmannadsystemstechnology, Mai 2021

Drone sous-matin KATFISH de Kraken Robotics embarquant un dispositif ATR. Source: Ocean News and Technology

Concrètement, des capteurs sonar performants peuvent être utilisés pour collecter les données, qui sont ensuite traitées et analysées par l'IA lors de scénarios d'attaques ou de surveillance sous-marine.

UN GAIN DE PUISSANCE DANS LES STRATÉGIES DE DÉFENSE MILITAIRE

L'IA et le *Machine learning* sont de plus en plus utilisés dans les stratégies militaires mondiales en raison de leur capacité à traiter et à analyser de grandes quantités de données avec une précision et une rapidité accrue. Ces technologies contribuent à accroître la sécurité des soldats et sont efficientes dans la prévention des attaques et des mouvements ennemis.

En matière de défense, ces nouvelles technologies peuvent tout d'abord être utilisées pour analyser les données recueillies par les radars, les satellites et les drones pour détecter les menaces potentielles. Les modèles d'IA sont capables d'évaluer les vulnérabilités et les risques liés à des situations spécifiques. Les algorithmes de détection de cibles sont quant à eux éduqués afin de repérer des véhicules militaires, des navires ou des avions qui pourraient représenter une menace pour la sécurité. De même, ces algorithmes d'analyse de comportement permettent d'identifier les modèles d'activité qui pourraient indiquer des activités illégales, telles que des infiltrations ennemies ou des attaques potentielles. Certains logiciels de surveillance utilisent des algorithmes d'apprentissage automatique pour identifier les véhicules militaires, les navires et les avions qui pourraient représenter une menace pour la sécurité. Le système utilise des données radar et d'autres capteurs optiques pour collecter des informations sur les cibles potentielles, puis les compare à des bases de données d'images de cibles connues. Ces systèmes sont alors capables de détecter des cibles à longue distance et en temps réel, permettant aux forces militaires de prendre rapidement des mesures pour contrer les menaces potentielles et de réduire les fausses alarmes.

Ces mêmes logiciels, en utilisant des techniques d'apprentissage supervisé d'IA, sont désormais entraînés à partir de données historiques, pour détecter automatiquement les menaces d'origines humaines en temps réel. Certains algorithmes sophistiqués de reconnaissance peuvent être formés sur des ensembles de données d'images radar pour identifier des formes et des structures spécifiques qui pourraient indiquer la présence d'objets ou de personnes intrus, notamment afin de détecter des personnes se trouvant à bord de bâtiments navals. Certains algorithmes sophistiqués de reconnaissance d'images de ces systèmes peuvent identifier, grâce à l'IA, des formes et des structures spécifiques associées aux corps humains et les distinguer des autres formes présentes dans les images radar.

Enfin, en alliant l'IA et les données de géolocalisation fournies par des systèmes spatiaux, il est possible de développer une nouvelle forme de surveillance continue des zones géographiques spécifiques, telles que des frontières ou des zones de conflit. Le mécanisme de surveillance intégré Eurosur, utilisé par l'Agence européenne de garde-frontières et de garde-côtes (Frontex)[6] pour surveiller les frontières de l'Union européenne utilise une combinaison dans les communications des technologies telles que les radars, les caméras, les capteurs infrarouges et les drones, ainsi que des algorithmes d'IA, ce système contribue à détecter les mouvements suspects et les activités illégales aux frontières.

Une des salles de contrôle du dispositif EUROSUR de Frontex. Source : Frontex

[6] "European Border Surveillance System (EUROSUR)" - Europa.eu

Il est utilisé pour prévenir les activités de trafic de drogue, de contrebande et d'immigration illégale mais il pourrait être utilisé dans l'hypothèse d'une guerre territorialisée sur le vieux continent. En ces termes, il serait possible d'analyser le comportement des ennemis et des forces hostiles, en utilisant des données historiques pour déterminer les tendances et les modèles comportementaux des troupes ennemies.

CYBERGUERRE : QUAND L'INTELLIGENCE ARTIFICIELLE PREND LES ARMES

Si l'intelligence artificielle est capable d'améliorer la pertinence des armes d'attaque et des stratégies de défense, l'avènement de la cybercri--minalité lui donne un rôle nouveau et tout aussi important. En effet, l'IA est devenu depuis ces dernières années un facteur permettant aux cyberattaquants, qu'ils soit affiliés à un État ou non, de rendre leurs attaques plus précises et plus ciblées mais également permettant aux infrastructures réseaux militaires de se protéger plus efficacement.

UNE CYBERDÉFENSE PLUS IMPERMÉABLE ET PRÉDICTIVE

En matière de cyberdéfense militaire, le rôle que peut constituer l'IA dans la détection des cyberattaques et la réduction du risque de com--promission est lui aussi de plus en plus conséquent. Les algorithmes de détection d'anomalies peuvent contribuer à identifier les modèles de trafic de données qui sont inhabituels ou suspects, tandis que les algorithmes de classification peuvent être utilisés pour classifier le trafic réseau comme légitime ou malveillant.

Grâce à l'apprentissage autonome des logiciels intégrés, la cyberdéfense militaire peut mettre en place une analyse prédictive des menaces. Ces modèles prédictifs contribuent à anticiper les failles de sécurité et les points faibles, en permettant aux équipes de sécurité de se préparer à des attaques potentielles et d'agir rapidement pour empêcher les cybercriminels d'exploiter les vulnérabilités dans l'infrastructure du réseau informatique militaire.
De surcroît, l'intelligence artificielle, dans son intégrité même, peut être utilisée pour renforcer la sécurité des réseaux militaires en permettant aux équipes de sécurité de prendre des décisions plus rapides et plus précises. Notamment dans la classification et le tri des alertes de sécurité en fonction de leur niveau de gravité, ce qui permet ainsi aux équipes de sécurité informatique militaire de se concentrer sur les menaces les plus critiques et d'agir rapidement voire instantanément pour les neutraliser. Lors de conflits armés, le timing avec lequel les menaces sont traitées est primordial pour une cyberdéfense efficace.

Si ces nouvelles technologies accentuent l'imperméabilité des réseaux informatiques militaires et sont favorables à la cyberdéfense, l'IA et le *Machine learning* sont des éléments constitutifs des cyberattaques actuelles, les rendant plus saillantes et plus impactantes. Ces cyberattaques modernes présentent un risque désormais majeur dans les conflits militaires mondiaux.

DES CYBERATTAQUES PLUS PRÉCISES ET DESTRUCTRICES

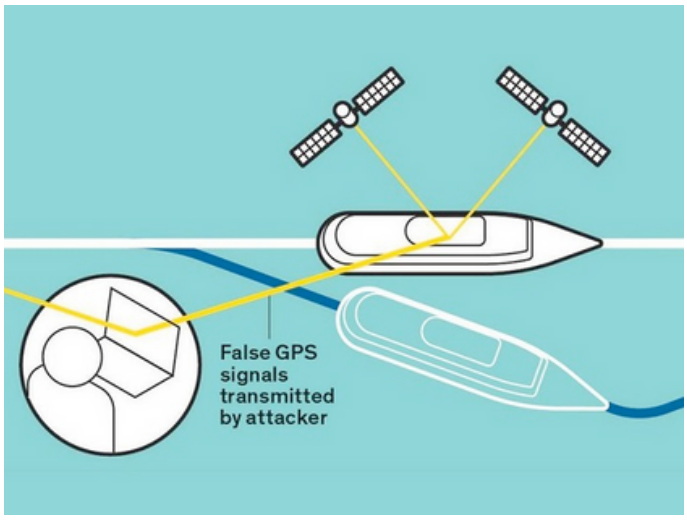
L'IA est en train de révolutionner les cyberattaques militaires, en fournissant aux acteurs malveillants des outils plus précis, plus efficaces et plus indé--tectables. Grâce à l'IA, les auteurs de cyberattaques sont capables de déceler plus facilement les vulnérabilités dans les systèmes de défense militaire, d'automatiser les processus d'attaque, de contourner les mesures de cyberdéfense mises en place et de rendre les intrusions encore plus imperceptibles et complexes à contrer.

La première tâche qui peut être attribuée à des logiciels dotés d'IA est l'identification des failles dans les systèmes de défense. Cette approche est connue sous le nom d'analyse de vulnérabilités automatisée et est largement utilisée dans les systèmes de sécurité pour identifier ces dernières. Les attaquants, grâce à cette technologie, sont désormais capables de développer

des systèmes de détection les vulnérabilités et les potentiels *backdoors* dans les infrastructures réseaux militaires. Il s'agit plus précisément de systèmes qui sont de taille à analyser des millions de lignes de code en quelques heures seulement, ce qui aurait pris des semaines, voire des mois, pour un expert en cybersécurité.

Dans un second temps, l'IA peut également être utilisée dans une pratique d'automatisation des processus d'attaque, permettant aux cybercriminels de lancer des attaques plus rapides et efficientes. Les attaques automatisées peuvent être personnalisées en fonction des données collectées sur les systèmes de défense, ce qui augmente les chances de succès de cette dernière. Cette automatisation, associée à des techniques sophistiquées de brouillage et de détection des mesures de sécurité, peut permettre à des algorithmes d'apprendre à reconnaître les signatures des mesures de sécurité et à les éviter. Ces technologies peuvent également être mises à l'œuvre dans des tentatives de *spoofing*. Pouvant être traduit par une tentative d'usurpation des signaux, cette cyberattaque a pour but de corrompre et réduire l'intégrité des informations échangées entre les stations terrestres et les satellites. Concrètement, le *spoofing* a pour but de remplacer le signal sain par un faux signal. Pendant que le récepteur continue de fonctionner, l'intrusion est presque indétectable. Entre autres, un *hacker* pourrait contrôler le système de navigation (GNSS) d'un bâtiment naval en verrouillant son cap sur un faux signal.

Enfin, l'IA peut rendre les cyberattaques plus indétectables. Grâce au *Machine learning*, des logiciels malveillants sont capables d'imiter les comportements normaux des utilisateurs, brouiller les données de surveillance et les journaux d'activité, rendant encore plus indétectables les intrusions, en se fondant dans le paysage numérique de la structure réseau militaire. Ces stratégies s'organisent autour de techniques de pointe comme la génération de trafic réseau artificiel, l'imitation d'empreinte numérique, la falsification de journaux d'activité ou encore de l'utilisation de techniques d'encodage ou de chiffrement, dans le but de masquer des données sensibles et rendre plus difficile leur détection.



Visualisation simplifiée d'une usurpation des signaux dans les communications GPS d'un bâtiment naval.
Source : Opex360.com

L'IA COMME OUTIL DE DÉSINFORMATION ET SURVEILLANCE EN TEMPS DE GUERRE

Si l'intelligence artificielle peut être utilisée pour soutenir des efforts de guerre en fournissant des outils de renseignement et d'analyse de données, elle peut également être utilisée pour propager de la désinformation et de la propagande. Les gouvernements et les groupes militaires sont capables, grâce à des *bots*[7] de réseaux so--ciaux, de propager de la désinformation et, de la même manière, d'influencer l'opinion publique en leur faveur. Ces bots peuvent être programmés pour diffuser des messages spécifiques, y compris de fausses informations et des théories du complot. Mais en matière de fausses informations, c'est bien les *deepfakes* qui deviennent de plus en plus pertinents.

DEEPFAKE : DES ARMES DE MANIPULATION MASSIVE

L'augmentation accrue des *deepfakes* en temps de guerre constitue une constante bien représentative de l'importance de l'IA dans l'in--fluence d'opinion publique et la décrédibilisation de l'ennemi. Les deepfakes sont des contenus médias artificiels créés à l'aide de techniques d'IA avancées permettant de concevoir des vidéos ou images synthétiques extrêmement authentiques alors qu'en réalité, elles sont entièrement fabriquées. En temps de guerre intraterritoriale, des groupes de cybercriminels utilisent cette technologie dans le but d'influencer l'opinion publique qui n'a, dans certain pays, qu'un accès très restreint à l'information et donc au *fact-cheking* (vérification des faits). Récemment, en plein conflit russo-ukrainien, la chaîne de télévision Ukraine 24 s'est vue être victime d'une cyberattaque en Mars 2022.[8] Les cybercriminels ont par la suite diffusé en pleine heure de grande écoute une deepfake du président ukrainien Volodymyr Zelinski Sur cette vidéo, le Président appelle les forces et civils ukrainiens à rendre les armes face à la menace russe.

Comparaison du réalisme du deepfake de Zlinski en Mars 2022.
Source : BiteFender

Une vidéo réaliste mais évidement créée de toutes pièces grâce à l'IA, dont les seuls buts étaient de semer le doute et de jeter un discrédit sur le Président ukrainien. Avec l'amélioration des logiciels d'IA, les *deepfakes* créées deviennent de plus en plus réelles et constituent un menace sérieuse à l'heure actuelle. En réponse à ces préoccupations, plusieurs organisations ont commencé à travailler sur des outils de détection de *deepfakes* pour aider à identifier les vidéos et les images synthétiques.

UNE SURVEILLANCE STRICTE PHYSIQUE ET NUMÉRIQUE

Enfin, les systèmes de reconnaissance faciale et de surveillance alimentés par l'IA peuvent être performants, dans le cadre de conflits intérieurs, afin de surveiller et suivre les mouvements des civils et des groupes d'opposition, ainsi que pour harceler les opposants politiques. En ce qui concerne les systèmes de reconnaissance faciale, ils sont souvent utilisés pour des applications de sécurité publique, tels que la surveillance des foules lors d'événements publics importants ou de manifestations. Cependant, ces mêmes technologies peuvent également être utilisées de manière abusive pour suivre les mouvements des civils et des groupes d'opposition. En Chine, par exemple, le gouvernement use de systèmes de reconnaissance faciale pour surveiller les minorités ethniques, telles que les Ouïghours, en utilisant une base de données de reconnaissance faciale pour suivre les déplacements et les activités de ces populations.[9]

[7] Les bots de réseaux sociaux, ou "social bots" en anglais, sont des programmes informatiques conçus pour interagir avec les utilisateurs des réseaux sociaux de manière automatique et autonome, en simulant le comportement humain.

[8] "Un deepfake du président ukrainien rendant les armes diffusé sur la toile" - Siècle Digital, Mars 2022

[9] "How China Is Using A.I. to Profile a Minority" - The New York Times, Avril 2019

La France vient quand à elle de voter une loi autorisant l'exploitation de la video à reconnaissance faciale sur l'espace publique des JO de Paris en y intégrant une analyse comportementale de l'image permettant de détecter un individu présentant une attitude non conforme à l'image physiologique qu'un individu decrait avoir s'il n'avait rien à se reprocher !

Quant aux systèmes de surveillance alimentés par l'IA, ils sont souvent utilisés pour surveiller les communications et les activités en ligne.

SenseTime, une des sociétés chinoises d'intelligence artificielle développant une technologie de reconnaissance faciale.
Source : Gilles Sabrié pour le New York Times

Les gouvernements les utilisent pour détecter les activités subversives, telles que la radicalisation en ligne et la planification d'attentats terroristes. Par ailleurs, ces mêmes technologies peuvent également être manipulées dans le but de harceler les opposants politiques. En Turquie, depuis 2018, le gouvernement use par exemple, des systèmes de surveillance alimentés par l'IA pour surveiller les médias sociaux et les activités en ligne des opposants politiques, entraînant l'emprisonnement de nombreux opposants au gouvernement.[10]

La présence croissante de l'IA dans les conflits modernes n'est plus à démontrer, et sa pertinence n'est plus à tester. Cette nouvelle technologie est utilisée à la fois pour améliorer l'efficacité des systèmes d'attaque et de défense militaires mais également pour créer de nouvelles menaces et de nouvelles manières de se défendre. Si l'IA ne cesse de s'améliorer chaque jour dans notre quotidien, elle se complexifie et opère un rôle préoccupant dans les enjeux de puissance entre entités influentes du monde. En fin de compte, l'influence de l'IA dans les opérations de cyberguerre ou de guerre conventionnelle dépendra de la manière dont elle est utilisée et des précautions prises pour prévenir les abus. Les acteurs qui en font usage se doivent de prendre des mesures pour éviter les dérives telles que la désinformation, la propagande et la surveillance outrancière. Parmi ces mesures, on envisage dans un futur proche, un renforcement de la réglementation, un renforcement des protocoles de sécurité ainsi que du niveau de formation des employés pour prévenir notamment les attaques de *phishing* et d'ingénierie sociale. On peut espérer voir la mise en place de protocoles de vérification d'identité et d'autorisation des utilisateurs d'IA, et assister au renforcement d'une collaboration entre les organisations publiques et privées pour développer des stratégies de cybersécurité efficaces.

En définitive, il est essentiel de maintenir un équilibre entre les avantages et les risques potentiels de l'utilisation de l'IA dans les opérations militaires, en veillant à ce que les avantages soient exploités de manière responsable et que les risques soient minimisés pour éviter les conséquences néfastes pour les utilisateurs et les populations civiles.

10 "How China Is Using A.I. to Profile a Minority" - The New York Times, Avril 2019

Rédaction par Alex Fabre et Frans Imbert-Vier
Édition avril 2023


UBCOM SWISS INTELLIGENCE AGENCY
CYBER PROTECTION AND SOVEREIGNTY