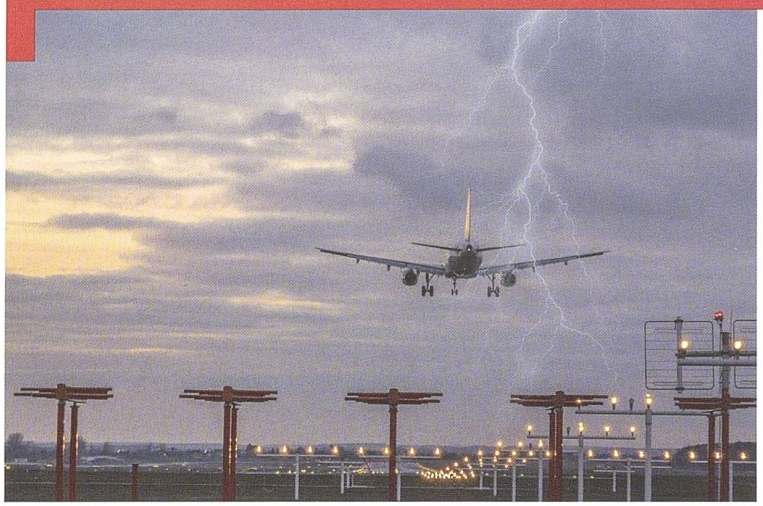
Zeitschrift: Revue Militaire Suisse
Herausgeber: Association de la Revue Militaire Suisse
Band: - (2024)
Heft: 5

Artikel: L'intelligence artificielle et le secteur aérospatial : aubaine ou risque?
Autor: Martel, Daniel Stanislaus
DOI: https://doi.org/10.5169/seals-1075557



Aviation

L'intelligence artificielle et le secteur aérospatial – aubaine ou risque ?

Daniel Stanislaus Martel
Directeur de la publication *Point de Mire*

« Chers passagers, ici votre avion. Nous avons atteint l'orbite basse. Dans les prochaines 26 minutes, vous vivrez l'apesanteur. » « Aviotaximat valide votre réservation d'un robot-taxi aérien automatique qui vous récupérera dans 10 minutes devant votre maison. » « Bonjour, cher pilote, je suis votre Helveticair Airbus A121-500 et je me réjouis de notre mission à Varna, près de la mer Noire. Veuillez donc m'autoriser à inviter les 48 voyageurs à l'embarquement. Je mets déjà la musique adaptée à ce groupe de vacanciers. » Voilà quelques scénarios inspirés de la science-fiction. Anticipée depuis des décennies sous la forme d'ordinateurs dotés d'une personnalité, l'intelligence artificielle (IA) est, dit-on, devenue réalité. Est-ce que l'IA est une opportunité, comme les uns disent, ou bien représente-t-elle un danger, comme les autres le craignent ? Qu'en est-il pour le secteur aérospatial ? Une chose est rassurante : l'avion autonome, donc sans contrôle humain, ne volera pas de sitôt.

Or les futurs imaginés ne sont pas tous encourageants. « Si vous n'arrêtez pas immédiatement de déconnecter mes caméras, menace l'ordinateur qui dirige le contrôle aérien au-dessus de l'Irlande, je détruis les 31 avions actuellement sous ma responsabilité. » « J'ai infiltré les plateformes collaboratives de tous les ingénieurs-développeurs de nos concurrents Airbus et Boeing. » « Depuis deux jours, c'est le chaos total au niveau des bagages dans tous les aéroports en Pologne. » « Je sais, c'est un nouveau virus intelligent et autonome qu'une organisation terroriste du Proche-Orient a introduit. » Ce sont d'autres situations typiques, négatives cette fois.

L'intelligence artificielle, c'est quoi ?

Le recours aux machines de calcul par les constructeurs remonte aux années 1930. Dès les années 1950, les compagnies aériennes ont employé des cerveaux électroniques. Les années 1960 ont vu les premiers automates s'occuper des réservations. Une décennie plus tard, les systèmes experts et de planification sont apparus. Les ordinateurs individuels ont rejoint le secteur aérospatial après 1983. La décennie suivante a été témoin de l'intégration de toutes ces solutions, avant que internet ne se tisse depuis les années zéro. Celui-ci a conduit à la dématérialisation des processus, du billetage à la documentation de vol des équipages. Maintenant, c'est l'heure de la virtualisation des procédures dans le secteur aérospatial.

En détail, l'IA est la prochaine étape des développements esquissés plus haut, et ce, pour plusieurs raisons. En premier lieu sont concernées les quantités de données infinies récoltées sur les avions, les passagers, le fret ou les aéroports. Il y a une décennie, la valeur de ces fichiers a été reconnue et les données massives, ou big data, sont devenues le trésor des opérateurs.

Vient ensuite l'importance croissante des réalités augmentées ou virtuelles en construction, en maintenance et en opération. En troisième lieu, les systèmes experts et d'aide à la décision avaient fait leurs preuves. La pression sur les coûts et les marges, quant à elle, a été à l'origine de solutions spécialisées. Ainsi, un nombre croissant de compagnies aériennes a développé des applications pour gérer les commandes de plateaux-repas à bord selon des valeurs statistiques de longue durée au lieu du nombre de passagers enregistrés.

Les programmes dits « d'intelligence artificielle » (IA) sont, de ce fait, des passerelles entre ces différents logiciels thématiques et les données spécialisées. Conçus pour fonctionner de manière autonome une fois lancés, ils puisent les données pour fournir notamment des aides à la décision.

Avantages et chances pour le secteur aérospatial 4.0

L'aérospatiale s'appuie d'ores et déjà sur l'IA. Selon Accenture, l'IA est désormais intégrée dans la recherche de l'efficacité des vols et de l'efficience des procédures, l'amélioration des opérations au sol et la réduction des nuisances sonores et climatiques. L'automatisation et l'autonomie de l'IA sont d'ailleurs bien appréciées. En construction aéronautique, cependant, elle n'est pas encore adoptée. Le contrôle aérien est également loin pour l'instant d'obtenir de réels appuis de cette nouvelle tech-

nologie. Ces exemples montrent que pour les décideurs aéronautiques, l'IA n'est pas une solution miracle à tous les défis, mais un outil de travail comme un autre ; d'où les différents degrés d'adoption. Son but est le gain de productivité global par la meilleure allocation des ressources, que ce soit au niveau de la simplification des réservations, des manœuvres pour mieux bénéficier de l'espace aérien, de l'évaluation des données microéconomiques de chaque vol, ou encore d'une meilleure gestion des travaux d'entretien et des stocks de pièces de rechange. Surtout, l'IA générera elle-même des quantités de données presque illimitées qui pourront être utilisées pour des scénarios et l'évaluation microscopique des performances de chaque membre d'une flotte.

Risques : Le classique des changements technologiques

Bien sûr, l'IA n'a pas fait que des heureux. Avant tout, elle conseillera impitoyablement de supprimer des emplois pour optimiser la rentabilité. Pour l'instant, elle connaît encore des limites évidentes d'un point de vue aérospatial. Tout d'abord, ses résultats effectifs et les améliorations restent en dessous des attentes. En découlera une désillusion amère. Ensuite, l'IA est juste aussi bonne que les données qu'elle pourra utiliser. Puis, se rajoutent les pannes à proprement parler. Ces dysfonctionnements peuvent être très dangereux, car l'institution ou société utilisatrice en fait des piliers centraux de son fonctionnement. Demeurent les risques de fuites de données, les éventuelles erreurs de manipulation et bien sûr le vol.

Malveillance dans l'imaginaire plutôt que dans le réel

Le public et même des experts associent souvent l'IA à des scénarios catastrophe, car, pour eux, elle est liée à la cyberguerre. Un premier champ d'action souvent imaginé est le sabotage des opérations. Des logiciels IA pourraient être introduits dans les réseaux de compagnies aériennes, d'aéroports ou d'autres organisations. Quant aux dommages qui résultent des intrusions, ils peuvent aller du vol de données à la répartition de fausses informations jusqu'à ces fameux sabotages. Pour les prestataires de contrôle aérien et surtout les constructeurs, les risques sont encore plus élevés. Si les vols de données sont encore « tolérables », la désinformation, notamment introduite dans des études de marché ou prospectives, est bien plus dangereuse. Même si, pour l'instant, aucune interférence n'a été prouvée, le sabotage sur des éléments de l'ingénierie cruciaux d'un avion s'avérerait fatal. Quant aux auteurs de tels actes, il est légitime de penser à des groupes terroristes, des activistes écologiques, des institutions étatiques et surtout des concurrents. Ce genre d'attaque peut d'ailleurs être organisé sous fausse bannière, ou *false flag*, pour nuire à un concurrent ou pour discréditer un mouvement politique.

Comment être prudent ?

Comme toute menace au potentiel de devenir un risque, l'IA doit être abordée dans la perspective de la lutte contre les risques. L'opérateur devra faire la distinction entre deux types de prévention : celle contre les défaillances techniques, d'une part, et celle contre les intrusions malveillantes, d'autre part.

Pour les premières, il s'agit d'appliquer les mesures de prudence ou de *derisking* que l'on prend pour tout autre outil, de processus ou de procédure. En font partie les formations initiales, les normes d'application ou d'utilisation, la capacité du personnel à maîtriser les dispositifs et l'autorisation d'accès aux systèmes et aux résultats. En d'autres termes, c'est une opération d'outillage industriel dans l'optique d'augmenter la productivité et, par là, l'efficience et l'efficacité.

En situation défensive, toutes les mesures doivent être prises dans une perspective d'opération criminalistique, voire militaire. L'IA est un élément de la cyberguerre ou criminel uniquement si elle est appliquée dans ce contexte. Les tactiques et méthodes de la guerre d'intrusion comme le repérage des traces digitales seront retenues.

Conclusion : Mais qu'est-ce qui est réellement nouveau ?

La perception de l'IA est largement basée sur l'angoisse, voire la panique. Certes, elle fait partie de la cyberguerre et est utilisée à des fins de désinformation, mais ce n'est pas tout. Il restera à découvrir si les polémiques récentes découlent d'une campagne d'intoxication ou de « panique orchestrée ». Sans fermer les yeux sur les véritables enjeux et dangers, le phénomène de l'IA paraît, à l'heure actuelle, largement surestimé, voire gonflé. Sans pour autant nier les véritables risques, il convient de clarifier certaines choses. En premier lieu, il est sûr que, comme tous les secteurs, celui de l'aérospatiale va être durablement et profondément transformé. À plus long terme, il va suivre l'évolution vers le monde 4.0.

Comme partout, il y aura des gains et des risques. Parmi les premiers, les analystes et prospectivistes énumèrent notamment l'aide à la fidélisation des clients et une expérience créée sur mesure ainsi que la flexibilisation continue des opérations dont celle accrue de l'allocation d'avions de taille optimisée pour les routes et les portes au sol. Sont prédites également la personnalisation des systèmes de divertissement et les premières tentatives d'avions avec un seul pilote aux commandes. Ce dernier point ne fera toutefois pas l'unanimité. Enfin, des systèmes experts et de visualisation pourront aider les enquêtes sur les accidents et leur quête d'une meilleure sécurité et sûreté.

Les côtés négatifs de l'IA s'amplifieront logiquement. Loin de la cyberguerre et de l'intox, les véritables dangers sont les pannes, les erreurs d'application et l'inflexibilité des solutions digitales et bien sûr l'absence de suivi cohérent. Se rajoute bien entendu l'utilisation malveillante de l'IA. Ces abus présentent un danger bien plus grand pour les institutions qui recourent à l'IA que les intrus ou manipulations pilotées par un Etat ou un compétiteur hostile. Or l'ultime décideur devra toujours rester l'humain, car lui (et bien sûr elle !) aura des capacités décisionnelles bien supérieures à toute ligne de code.

D. S. M.