Deloitte.

L'ère de la *convergence*[MC]

L'avantage de l'IA pour le secteur de la défense et de la sécurité

Introduction

De nos jours, les gens d'affaires ne peuvent plus ouvrir une revue ou parcourir leur fil d'actualité Twitter sans voir les mots données, intelligence artificielle, automatisation, Internet des objets, robots, machines et transformation. Ces mots évoquent des occasions qui doivent être saisies maintenant, car nous sommes à un tournant historique, où plus rien ne sera comme avant. À jamais.

L'IA devient la feuille de route pour naviguer dans l'univers en constante mutation des données. Pour en profiter, vous devez amorcer votre parcours dans le monde de l'évolution technologique.

Votre succès se résumera en un mot : *convergence*.

Ce qui se passe autour de nous – données partagées, engagement social, assistants numériques, plateformes infonuagiques, appareils connectés – n'est pas un combat entre l'homme et la machine, mais plutôt une collaboration entre humains qui est rehaussée par les machines qu'ils inventent. C'est une ère nouvelle.

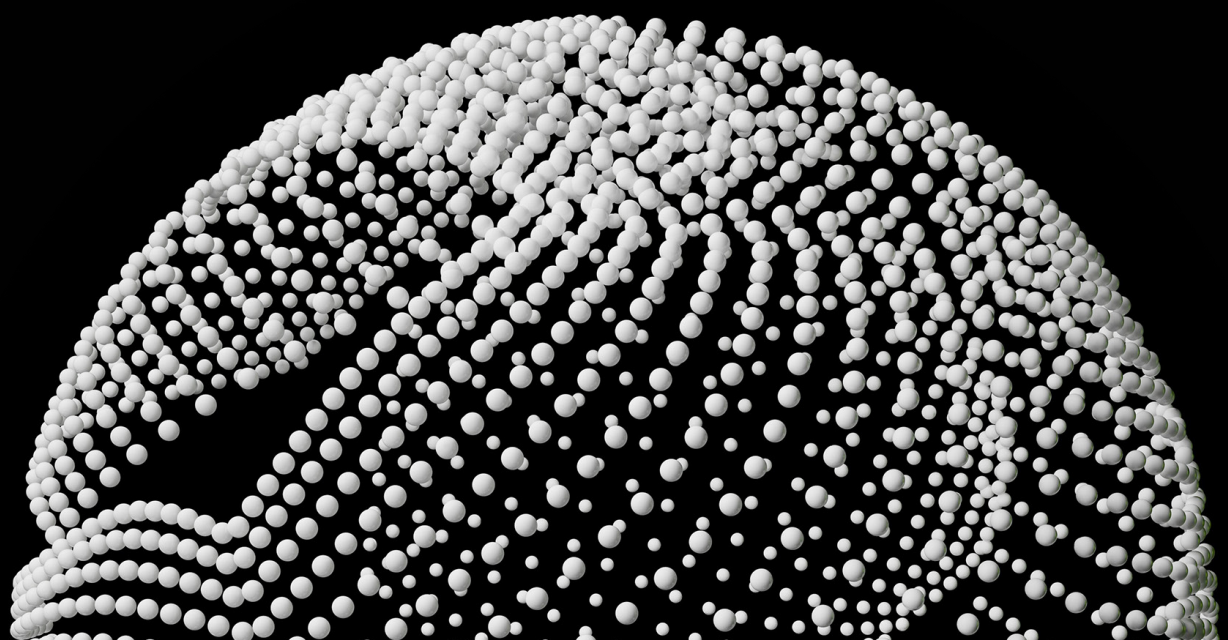
Si nous voulons être performants, concurrentiels et innovateurs, nous devons créer un avantage cognitif en exploitant le pouvoir de la *convergence* des données bien structurées avec la pensée conceptuelle, l'analytique et les machines.

Cela peut ressembler à un saut dans l'inconnu, mais ça ne l'est pas. La *convergence* est depuis longtemps le plus grand atout de l'humain. Nous la cherchons et en bénéficions. Nous l'utilisons pour créer des modèles d'affaires. Elle est même au centre de nombreuses grandes inventions, des municipalités à l'internet, en passant par la chaîne de montage. Deloitte possède les compétences diversifiées et interdisciplinaires, le sens des affaires et la vision nécessaires pour concevoir des solutions reposant sur l'IA et vous aider à adopter une attitude plus compétitive en intégrant l'IA.

Pour réussir dans l'avenir, il faut jumeler l'intelligence humaine et l'IA afin d'ouvrir la porte à encore plus de possibilités. Le potentiel est illimité.

Perturbations dans le secteur de la défense et de la sécurité

L'arrivée de l'IA risque de provoquer de profonds changements pour les gouvernements, notamment en améliorant l'expérience citoyenne, en stimulant la prospérité économique et en rehaussant la sécurité publique. C'est pourquoi les pays et les gouvernements du monde entier s'empressent d'adopter l'IA.



Tendances touchant les gouvernements

Nous remarquons tous la façon dont la technologie transforme nos activités quotidiennes, que ce soit l'apparition de Siri et d'Alexa, les recommandations personnalisées sur Amazon et Netflix et même la possibilité de faire venir un taxi ou de se faire livrer une commande d'épicerie en quelques clics. Les citoyens maîtrisent de mieux en mieux la technologie et en deviennent dépendants, tout comme les gouvernements. Les leaders gouvernementaux ont compris la nécessité, et les avantages, d'adopter une façon de penser qui met le numérique au premier plan. La quantité d'informations numériques générées connaît une croissance exponentielle, et le secteur public comme le secteur privé voient les avantages d'en faire une utilisation optimale.

En réponse à cette utilisation accrue du numérique, les gouvernements collaborent de plus en plus avec le secteur privé pour résoudre les problèmes complexes de l'ère numérique. Ils forment des partenariats pour réaliser des recherches de pointe et trouver les bonnes solutions à des problèmes uniques.

Pour avoir accès aux technologies appropriées, les gouvernements doivent composer avec un processus d'approvisionnement complexe. C'est pourquoi ils commencent à s'intéresser à d'autres types de modèles budgétaires et à des solutions d'approvisionnement agiles pouvant prendre en charge des projets pilotes, assurer une plus grande transparence du processus d'appel d'offres et intégrer toute une gamme de fournisseurs de services.

Faire plus avec moins

Le secteur de la défense et de la sécurité est un précurseur en matière d'innovation et de technologie. Les organisations de sécurité comptent parmi les plus grands producteurs et consommateurs de données; en proportion, elles détiennent déjà plus de données que les autres entreprises en raison de la nature de leurs activités. Ce secteur doit cependant relever de nombreux défis bien particuliers lorsque vient le temps d'obtenir des solutions, de les préparer, de les mettre en place et d'en généraliser l'utilisation. Étant donné la quantité d'actifs concernés – ressources humaines, véhicules, matériel, technologies, etc. –, les efforts nécessaires pour créer des solutions qui fonctionnent peuvent être immenses. De plus, les ministères doivent faire plus avec moins. Les budgets sont surveillés de très près. Pour répondre à la pression mondiale grandissante qu'ils subissent pour accroître les capacités, les ministères doivent utiliser leurs programmes et leurs ressources actuels de manière plus efficace et plus efficiente.

Il est temps de passer à l'IA

L'IA possède le potentiel d'élargir les horizons de façon complètement nouvelle. Dans le contexte de la croissance exponentielle des données et des capacités techniques, de l'évolution de la technologie et du pouvoir de traitement, et des investissements que les gouvernements effectuent dans la recherche et le développement en IA, le secteur public est prêt à mettre en œuvre de nouveaux outils qui contribueront à raccourcir le processus décisionnel. Qu'elles mènent leurs activités dans les domaines des forces armées, des services de police ou de la sécurité aux frontières, les organisations du secteur de la défense et de la sécurité doivent livrer bataille sur plusieurs fronts : exploiter leurs données, rationaliser leurs fonctions actuelles, mettre en œuvre de nouvelles technologies, tenir compte des questions d'éthique et se procurer les outils nécessaires à l'atteinte de leurs objectifs.

Les technologies perturbatrices et les capacités numériques constituent une arme à double tranchant : elles présentent une multitude de possibilités d'améliorer les fonctions de défense et de sécurité, mais elles offrent aussi une multitude de nouveaux moyens pour les criminels et les terroristes de perfectionner leur mode de fonctionnement. Les capacités des services de sécurité locaux et nationaux suffisent de moins en moins à la demande. À l'heure actuelle, la sophistication des sources de menace dans le monde progresse de manière exponentielle : des informations sont échangées sur le web invisible, il devient plus difficile d'enquêter sur les crimes commis, l'informatisation crée de nouveaux points d'attaque et les informations sont faciles à falsifier et à diffuser. Le monde est plus complexe que jamais. L'IA et les outils de traitement de l'information jouent un rôle déterminant en aidant les gouvernements à prendre les bonnes décisions de défense et de sécurité.

Occasions liées à l'IA pour le secteur de la défense et de la sécurité

Principaux domaines dans lesquels les technologies fondées sur l'IA peuvent servir à maximiser la valeur des actifs, à accroître les ressources et à procurer une plus grande valeur au secteur de la défense et de la sécurité.

	Détection	Planification	Opérations sur le terrain	Fonctions de soutien
Forces armées	Utiliser des systèmes d'IA pour recueillir des flux de données de surveillance et les analyser. Utiliser des capteurs intelligents pour repérer et suivre des objets ou du personnel.	Utiliser les données disponibles et des algorithmes d'apprentissage machine pour mieux prévoir les besoins en ressources pour les missions et les exercices d'entraînement ainsi que les coûts connexes.	Fournir des données en temps réel et des évaluations rapides pour améliorer l'issue des missions. Protéger les gens, les actifs et les renseignements.	Accélérer le processus d'approvisionnement et gérer les contrats avec les fournisseurs. Procurer des solutions de budgétisation intelligentes. Soutenir les fonctions des RH visant un recrutement intelligent, les services automatisés et les demandes relatives à la paie.
Services de police	Utiliser des algorithmes d'IA et des capteurs intelligents pour repérer des personnes et des objets dans des données numériques et des activités de maintien de l'ordre pour procurer une compréhension globale des scénarios de crise.	Utiliser les données disponibles et des algorithmes d'apprentissage machine pour mieux prévoir les menaces potentielles et déployer les ressources nécessaires.	Utiliser l'analyse fondée sur le raisonnement et des réseaux neuronaux pour gérer la collecte et l'interprétation des données sur des enquêtes en cours.	Accélérer le processus d'approvisionnement et gérer les contrats avec les fournisseurs. Procurer des solutions de budgétisation intelligentes. Soutenir les fonctions des RH visant un recrutement intelligent, les services automatisés et les demandes relatives à la paie.
Sécurité des frontières	Utiliser des algorithmes d'IA et des capteurs intelligents pour repérer les personnes et les objets pouvant présenter un danger aux postes frontaliers, aux postes de contrôle douaniers et à d'autres endroits.	Utiliser les données disponibles et des algorithmes d'apprentissage machine pour mieux prévoir l'activité des voyageurs, les menaces potentielles et l'affectation des ressources aux postes de contrôle de sécurité.	Utiliser des systèmes d'IA pour analyser les tendances et les habitudes à partir des données d'un voyageur et mieux repérer les activités suspectes.	Accélérer le processus d'approvisionnement et gérer les contrats avec les fournisseurs. Procurer des solutions de budgétisation intelligentes. Soutenir les fonctions des RH visant un recrutement intelligent, les services automatisés et les demandes relatives à la paie.

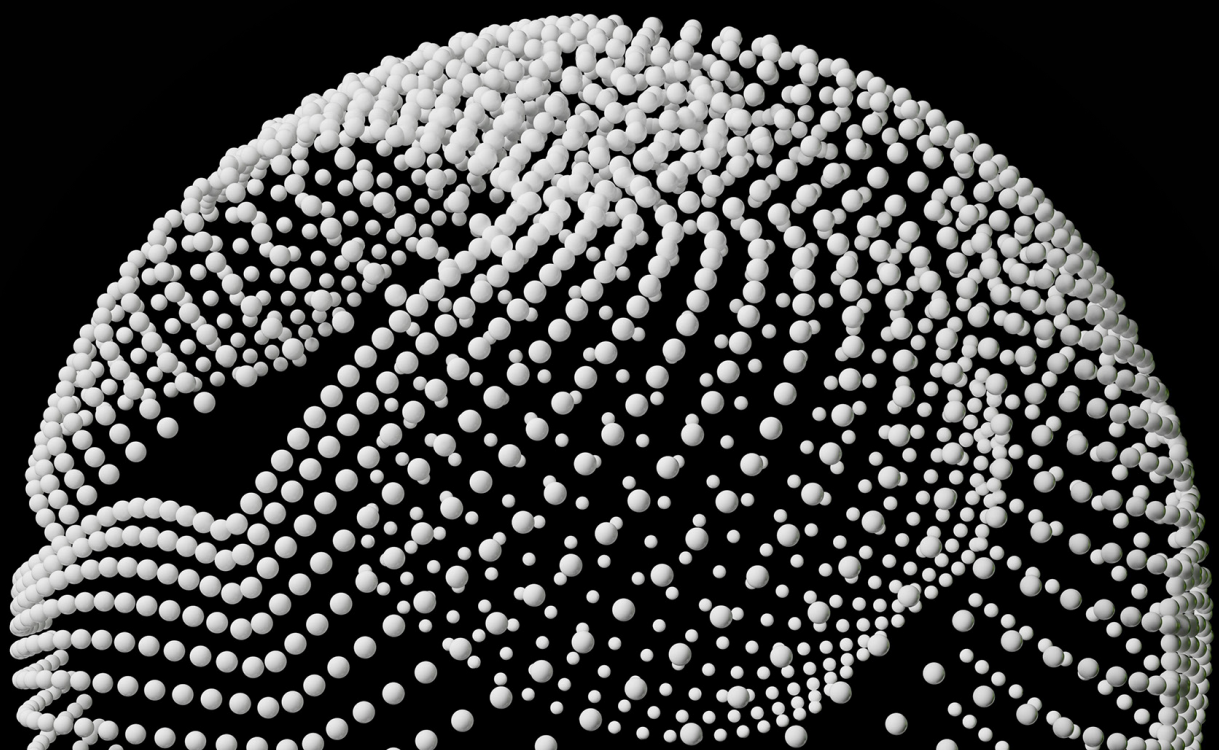
Occasions liées à l'IA pour le secteur de la défense et de la sécurité

L'éventail d'occasions que l'IA procure au secteur de la défense et de la sécurité est très large. La prolifération des données produites et recueillies permet d'obtenir une vision globale de l'état actuel et futur des opérations. En recourant à l'IA pour recueillir et compiler des données, les organisations sont en mesure de trier des montagnes d'informations, de déceler des interactions complexes et d'intégrer les résultats obtenus dans des analyses ainsi que dans la planification de scénarios prévisionnels[1].Des algorithmes d'apprentissage machine et des réseaux neuronaux complexes procurent des évaluations en temps réel pour soutenir les opérations critiques sur le terrain.

Les véhicules autonomes utilisant l'IA effectuent non seulement des activités de sauvetage, mais aussi des opérations à distance qui protègent des vies humaines. L'automatisation intelligente permet de réduire les tâches administratives associées à plusieurs rôles, notamment dans les services de soutien où les processus prennent souvent beaucoup de temps. Plus encore, la collaboration entre l'IA et l'être humain permet d'éliminer les activités non essentielles à faible valeur ajoutée qui détournent les gens de la mission principale, peu importe le rôle qu'ils jouent dans les opérations : planification et préparation, intervention sur le terrain ou soutien logistique.

Le présent rapport explore les possibilités et le potentiel de l'IA dans le secteur de la défense et de la sécurité, plus précisément en ce qui concerne les forces armées, les services de police et la sécurité des frontières. Il met en lumière les principaux éléments à considérer pour l'utilisation de l'IA et l'infrastructure requise pour mettre en œuvre les applications à grande échelle.

De nouvelles solutions avec de nouvelles approches



Forces armées

De la planification des missions à la technologie des capteurs, sans oublier la surveillance par drones et même les véhicules autonomes, les organisations militaires recherchent des moyens d'utiliser l'IA pour obtenir un avantage déterminant, tant pour leurs opérations que pour leurs fonctions de soutien.

L'occasion

Une quantité phénoménale de données de surveillance sont recueillies. Seule une petite portion de cette information est pertinente pour les opérations; pourtant, selon une estimation, la quantité de données recueillies uniquement par les drones militaires et d'autres technologies de surveillance a augmenté de 1 600 % entre 2001 et 2011[2]. Le problème consiste à trier toute cette information pour en extraire ce qui est réellement utilisable. L'intégration de l'IA à la collecte et à l'interprétation des flux de données de surveillance des satellites et des drones peut permettre de bien comprendre les facteurs en cause dans un conflit ou une crise[3], et ce, par le recours à des modèles d'IA et à l'analyse des tendances pour repérer des activités qu'un observateur humain pourrait ne pas considérer comme des menaces. Ces ensembles de données peuvent comprendre des données de missions passées, des facteurs environnementaux et cartographiques et des connaissances humaines sur le terrain recueillis par des agents de renseignements.

L'utilisation de ces ensembles de données globales est essentielle dans plusieurs situations, que ce soit pour recueillir des renseignements lors d'opérations ou planifier des scénarios militaires à tous les niveaux de commandement. Les ensembles de données permettent, par exemple, de recueillir et d'analyser l'opinion de la collectivité locale sur la présence militaire, notamment en extrayant des données des médias sociaux, et d'élaborer des stratégies pour lutter contre les campagnes de désinformation et les idées fausses. L'IA peut aussi entrer dans la planification de scénarios militaires à tous les niveaux de commandement – des commandants de la force opérationnelle aux compagnies et pelotons individuels qui déterminent les conditions de leur élément de mission. Une meilleure planification de la procédure de combat au moyen de l'IA fait en sorte que les ressources sont utilisées de la manière la plus avantageuse possible dans un contexte de mission.

La collecte et l'opérationnalisation de données pour soutenir les opérations militaires touchent bien plus que les seules activités de la mission principale. Les services de soutien que la fonction des ressources humaines fournit sont uniques aux organisations militaires. Dans les forces armées, les RH comportent nombre d'occasions de transformer l'expérience des soldats. Les agents de recrutement doivent aussi disposer de meilleures stratégies pour attirer les bons candidats. Des statistiques sur la façon dont les membres les plus performants ont été recrutés, les étapes précises où surviennent les départs et leur motif exact, ainsi que les raisons pour lesquelles certains font toute leur carrière dans les forces armées constituent de précieux ensembles de données pouvant servir à établir des stratégies pour cibler les candidats qui s'engageront à long terme. Quand un candidat est recruté, les RH voient à sa santé et à son bien-être. L'analyse des données sur les blessures et les maladies fréquentes, la durée des congés de maladie et le coût des soins, ainsi que des statistiques sur les problèmes de santé mentale, entre autres, procurent des renseignements permettant d'élaborer une approche plus axée sur l'être humain en matière de soins offerts au personnel et à leurs personnes à charge.

Des défis sans pareils

L'application de l'IA dans le domaine militaire comporte des défis uniques en leur genre. La collecte d'une grande quantité de données suppose aussi que l'on tienne compte de la qualité des données, de l'endroit où elles sont stockées, des personnes qui y ont accès, de leur classement et de leur centralisation. Les systèmes et les technologies actuels présentent des problèmes intrinsèques de compatibilité avec la façon dont les données sont saisies et traitées. Les limitations de l'infrastructure technique compliquent par conséquent la mise en œuvre de l'IA[4]. En outre, les organisations militaires utilisent des réseaux fermés, ce qui rend encore plus complexe l'accès aux renseignements au moyen des nouvelles technologies. Les fournisseurs potentiels d'IA doivent se demander comment ils peuvent intégrer l'infrastructure de réseau actuelle afin de produire les renseignements pertinents en temps réel.

Le processus d'approvisionnement peut également être une entrave à l'adoption de nouvelles solutions dans le secteur militaire. Dans le secteur public, en effet, le cahier des charges est en général clairement défini; or, les solutions d'IA et les nouvelles capacités, elles, peuvent être difficiles à définir. Passer en revue les fournisseurs potentiels peut prendre beaucoup de temps, parfois des mois, et tout changement au sein de la direction risque de se traduire par la reprise de l'ensemble du processus. Pour résoudre ce problème, les organisations militaires cherchent à créer des mécanismes d'approvisionnement plus agiles grâce auxquels un partenaire choisi pour plusieurs années participe à l'élaboration de projets pilotes et de cas d'utilisation qui créent une valeur croissante tout au long de leur cheminement vers l'IA.

Ces types de solutions prennent encore plus d'importance lorsque vient le temps de mettre en œuvre l'IA dans des fonctions de soutien aux forces armées, comme les services des finances ou des RH. Dans ces services, les robots conversationnels permettent un accès plus rapide aux renseignements sur les antécédents médicaux et les prestations, et l'automatisation intelligente permet de traiter les documents de paie de façon plus rapide et plus efficace, ce qui libère les fonctionnaires pour qu'ils se consacrent à des tâches de plus grande valeur. Lorsque les processus appropriés sont en place, l'IA peut transformer les opérations militaires tactiques et la composition des équipes dont les membres travaillent dans l'ombre pour les soutenir.

Les possibilités qu'offre l'IA pour les opérations militaires

Renseignements et données
Intégration de l'IA à la collecte et à l'interprétation des flux de données de surveillance des satellites et des drones pour une vision plus claire des facteurs en cause dans un conflit ou une crise, prenant en compte les données de missions passées, des facteurs environnementaux, etc. Utilisation de véhicules autonomes, comme des sous-marins et des machines terrestres, munis d'algorithmes d'apprentissage par renforcement pour effectuer des opérations de reconnaissance et trouver des cibles[5].

Logistique et planification de la mission et vision claire de l'objectif
Regroupement de données sur l'environnement, les actifs et les missions passées pour mieux prévoir les scénarios de mission et assurer une affectation profitable des ressources et la coordination entre les multiples missions, opérations et forces opérationnelles. Choix de l'emplacement optimal pour les bases et les chemins d'évacuation et d'approvisionnement pour les activités militaires et humanitaires.

Maintenance prévisionnelle des actifs et confiance
Utilisation de la technologie des capteurs et de la vision par ordinateur pour déceler des failles et des pannes de système dans le matériel avant qu'elles ne surviennent. Recours à l'apprentissage profond et à des algorithmes de planification pour établir les calendriers de maintenance selon les normes opérationnelles des diverses composantes afin de réduire le nombre d'accidents et les retards imprévus. Regroupement et analyse des actifs immobiliers pour créer de meilleures stratégies de gestion et de maintenance.

Opérations améliorées et précision
Utilisation de la technologie des capteurs pour suivre les déplacements des compagnies et repérer rapidement les objets inconnus sur le terrain, ce qui soutient la prise de décisions éclairées. Recours à des véhicules autonomes pour accomplir des tâches nécessaires à la survie des soldats blessés sur le terrain.

Opérations dans le spectre électromagnétique et précision

Une opération de guerre dans le spectre désigne l'utilisation militaire du spectre électromagnétique (« EMS ») pour repérer des forces en présence, perturber les communications de l'ennemi et désactiver ses radars[6]. Les opérateurs de l'EMS reçoivent une multitude de signaux sur leur tableau de bord, dont la plupart ne sont pas critiques. Ils sont responsables de déchiffrer les signaux et de déterminer quelle mesure prendre. La technologie de la guerre électronique évolue, et l'IA permet une analyse plus rapide des données provenant des capteurs ainsi que l'établissement de corrélations entre les points de données en temps réel.

L'utilisation de l'IA pour filtrer le bruit entrant allège la tâche de l'opérateur et lui permet de se concentrer sur les signaux importants[7].

Services de police

Le grand public est très sensible aux comportements et aux activités des agents de police. Entre les vidéos diffusées en direct par les passants, l'intérêt accru que leur portent les médias et leurs interactions constantes avec les citoyens, les agents de police sont parmi les fonctionnaires les plus étroitement surveillés.

L'occasion

Toutes les technologies numériques qui tiennent dans la main et le foisonnement des données générées représentent des occasions intéressantes de mobiliser le grand public de manière positive, en utilisant cette information pour améliorer la sécurité publique. Les services de police montrent un intérêt croissant pour la création de portails de services pouvant servir à diverses fins. Ces portails pourraient constituer des plateformes pour la prochaine génération de communications avec le 911, étendant le rôle du 911 et des répartiteurs et permettant aux citoyens de transmettre des nouvelles en temps réel sous la forme de textos, de photos ou de vidéos, ce qui permettrait de recueillir beaucoup d'informations sur un incident de sécurité publique. L'intégration de l'IA à ces plateformes permettrait d'opérationnaliser ces données et d'en faire le tri pour tracer un portrait plus exact de la crise. L'IA permet aux répartiteurs de classer les interventions policières par ordre de priorité plus efficacement grâce au regroupement de plusieurs sources d'information sur un seul incident, ainsi que de fournir des mises à jour aux policiers en mouvement, et même d'assurer la coordination avec d'autres services d'urgence ou d'autres organismes. Les services de police pourraient s'adresser au public pour appuyer des événements comme les alertes Amber, ou pour obtenir son aide et le tenir informé.

La façon dont les services de police recueillent, gèrent et échangent leurs données change aussi. Les forces policières cherchent des moyens d'utiliser des portails de données ouvertes pour divulguer des données auparavant confidentielles ou contrôlées au grand public pour qu'il s'en serve de différentes façons et pour fournir au secteur privé des renseignements et des cas d'utilisation des données et d'application de l'IA. Les fournisseurs de caméras d'intervention prennent des mesures pour profiter de la prolifération des données dans le secteur en changeant leur modèle d'affaires de manière à proposer des capacités de collecte et de gestion des données, une option d'approvisionnement séduisante pour les organisations qui ont de la difficulté à coordonner les services de plusieurs fournisseurs pour la gestion des données.

Des défis sans pareils

Les occasions qu'offrent les données se multiplient, tout comme les inquiétudes que suscitent la manière dont ces données sont utilisées et l'endroit où elles sont. Des pressions s'exercent en faveur de l'utilisation des outils et des technologies d'IA, d'abord pour assurer la sécurité publique et donner de meilleurs résultats, mais aussi pour éliminer les partis pris possibles et assurer la transparence des solutions en intégrant des mesures de sécurité et de confidentialité. La technologie joue un rôle de plus en plus important, c'est pourquoi certains agents et services de police font l'objet de poursuites pour violation des droits de la personne et de recours collectifs qui ont mené à l'abandon de logiciels et d'outils. La confidentialité des données soulève aussi des préoccupations : des poursuites peuvent être déposées, et certaines l'ont été, contre des organisations qui ont obtenu des données personnelles, comme la photo d'une personne dans le cadre d'une enquête, et qui ont ensuite utilisées ces données personnelles recueillies aux fins d'une autre enquête, pour un usage autre que celui pour lequel elles avaient été recueillies. Ces poursuites remettent en question l'utilisation des images des caméras d'intervention obtenues par un agent qui circule dans différents environnements en recueillant de grandes quantités d'informations. On se demande aussi quelles données peuvent être utilisées en tenant compte de la confidentialité des données personnelles. Il y a un intérêt grandissant pour l'IA, mais les questions d'éthique restent à l'avant-plan du débat.

Pour répondre à ces préoccupations, des éléments de sécurité doivent être intégrés aux solutions d'IA dès le départ, et non après coup. Il faut tenter de comprendre les facteurs qui ont mené à un événement touchant la sécurité. Les services de police sont prêts à utiliser l'IA, mais il y a une opposition naturelle entre l'adoption de cette technologie et l'existence d'un cadre de gouvernance permettant d'éviter les conséquences involontaires. C'est en ce sens que le *Règlement général sur la protection des données* de l'Union européenne inclut un énoncé stipulant qu'une personne doit avoir le droit de ne pas faire l'objet d'une décision ayant un effet juridique prise sur le seul fondement d'un traitement automatisé[8]. C'est pourquoi il est si important que l'IA et les êtres humains collaborent pour obtenir les meilleurs résultats possible, en s'assurant que l'IA n'a pas de composante cachée qui ne peut être expliquée. Cette collaboration entre l'être humain et la machine est promise à un brillant avenir. En effet, le roulement important à la direction des services de police s'est traduit par l'entrée en poste de personnes plus au fait des technologies et qui en connaissent les effets perturbateurs.

Malgré cela, l'adoption de l'IA par les services de police nécessite la mise en place d'un cadre d'éthique prenant en compte la façon dont l'IA est utilisée, ce pour quoi elle l'est et la façon de traiter la transparence et les partis pris inhérents aux algorithmes.

Les possibilités qu'offre l'IA pour les services de police

Enquêtes et preuves
Utilisation de l'analyse fondée sur le raisonnement et des réseaux neuronaux pour mieux gérer la collecte et l'interprétation des données des enquêtes, notamment par la numérisation des documents papier, et ainsi trouver des liens entre des éléments de preuve, traiter les données provenant des médias et repérer les activités criminelles. Regroupement d'ensembles de données provenant de plusieurs services d'urgence afin d'éclairer les enquêtes et les activités policières.

Administration et compréhension
Réduction du fardeau administratif des agents de police grâce à l'automatisation de différentes tâches de bureau et de conformité. Accès à des fonctions de recherche intelligente qui fournissent rapidement des résultats et les fichiers correspondants pendant le processus d'inculpation d'une personne. Soutien aux fonctions de recrutement pour cibler les qualités, l'origine et les compétences voulues, surtout dans les régions où la population n'a pas confiance dans le corps policier.

Affectation des ressources et données
Utilisation des données disponibles pour mieux prévoir les menaces et les scénarios et ainsi mieux déployer les ressources policières et assurer la sécurité du public et l'utilisation efficace du personnel de soutien.

Service de police et savoir-faire
Utilisation de la technologie des drones et des capacités de reconnaissance d'images pour localiser les personnes disparues, gérer les scènes de crime et faciliter les enquêtes médico-légales. Utilisation de capteurs intelligents pour entendre les coups de feu, repérer les plaques d'immatriculation signalées et enregistrer les emplacements pendant que les policiers sont sur la route.[9] Collecte de preuves auprès du public dans les situations d'urgence, analyse en temps réel et sélection des renseignements pertinents.

Enquêteurs de police et confiance

En raison de l'utilisation accrue de la vidéo sous diverses formes – images TVCF, caméras-témoin et caméras d'intervention – les agents de police et les enquêteurs doivent examiner ce qui représente parfois de nombreuses heures d'images vidéo à la recherche d'un élément d'information important. Toutefois, selon certaines études, après avoir regardé un écran pendant plus de 20 minutes, une personne perd 95 % de sacapacité à détecter des événements[9]. Grâce à l'analyse fondée sur le raisonnement et aux réseaux neuronaux, un enquêteur peut utiliser l'IA pour :

- désigner une zone spécifique dans une vidéo pour repérer les changements qui s'y produisent, comme la disparition d'articles dans un magasin de détail;
- repérer des éléments ou des comportements anormaux, comme une voiture qui roule vite et grimpe sur un trottoir ou une valise abandonnée dans un lieu public;
- rechercher des éléments d'information précis, comme une marque et un modèle de voiture ou les vêtements que portait une personne disparue.

Sécurité des frontières

Aux États-Unis, le taux de départ des agents assurant la sécurité des frontières est deux fois plus élevé que celui des autres personnes chargées de l'application de la loi, la perte de moral et les mauvaises conditions de travail étant le plus souvent mentionnées comme motifs [10, 11]. En facilitant la tâche des agents grâce à l'IA, les organismes chargés de la sécurité des frontières pourraient accroître l'efficacité et l'efficience de leur personnel essentiel.

L'occasion

L'intégration de l'IA aux tâches des agents pourrait fournir à ceux-ci une aide indispensable pour repérer rapidement les personnes, les marchandises et les activités présentant un danger. L'affectation du personnel de sécurité a une incidence importante sur les ressources nécessaires pour patrouiller dans les zones de passage des frontières. En utilisant des capteurs intelligents et des ensembles de données intégrées sur les tendances migratoires, les passages aux frontières, les populations, l'environnement, etc., l'IA pourrait aider les agents de sécurité et permettre de réaffecter ou de déployer directement du personnel vers des zones frontalières où leur présence serait plus utile[12].

L'IA peut aussi servir à améliorer des systèmes existants, comme les appareils de détection à rayon X pour l'examen des bagages, des paquets et des colis. Grâce à la vision par ordinateur et aux algorithmes d'apprentissage machine, des marchandises dangereuses peuvent être repérées de manière plus précise et constante, ce qui réduit le nombre de tâches manuelles et le risque d'erreur humaine que suppose l'examen détaillé des images numérisées par les agents des services frontaliers.

Une foule de données sont recueillies chaque jour, mais souvent, elles n'ont aucune valeur tout simplement parce qu'elles se trouvent à des endroits disparates. L'intégration d'ensembles de données auparavant cloisonnés permet de révéler des liens qu'un être humain ne peut pas voir, mais que l'IA trouve. Les systèmes d'IA peuvent recueillir des données sur un voyageur particulier – formellement identifié par biométrie – qui traverse souvent la frontière, chaque fois accompagné d'un enfant portant un nom différent. Cette information pourrait ne pas être signalée immédiatement à un douanier. Mais en procédant au suivi et à l'analyse de ces données pratiquement en temps réel, un système d'IA pourrait indiquer à un agent des services frontaliers que ce voyageur doit faire l'objet d'une enquête plus approfondie parce qu'il semble faire la traite de personnes[10]. La vision au moyen d'appareils d'IA pourrait aussi faciliter cette enquête approfondie grâce aux caméras à infrarouge et aux systèmes de reconnaissance du débit sanguin qui permettent de déterminer si une personne ment. Selon certaines études, l'être humain est capable de détecter un mensonge dans environ 54 % des cas, alors que la précision de l'IA est de plus de 80 %[10]. Ces méthodes continuent d'être perfectionnées par l'apprentissage machine et l'intégration d'une quantité croissante de données. Les recherches semblent prometteuses, mais la question de la validité des détecteurs de mensonges reste au cœur du débat sur la mise en œuvre de ce type de technologie. On ne sait pas encore si cette technologie jouera un rôle dans la sécurité des frontières; tout comme d'autres aspects de l'application de la loi, elle comporte des enjeux dont il faudra tenir compte.

Des défis sans pareils

L'utilisation de la biométrie et des applications de reconnaissance faciale comporte de nombreux avantages, dont l'amélioration de la circulation des passagers dans les aéroports, ce qui permet au personnel de sécurité de se concentrer uniquement sur certaines personnes[13]. Il faut toutefois tenir compte des partis pris inhérents aux algorithmes utilisés pour entraîner les modèles sur lesquels sont fondés les logiciels de détection. C'est pourquoi il est si important de s'assurer que de nouvelles données sont régulièrement utilisées pour entraîner les modèles, ce qui augmente l'exactitude et la fiabilité des résultats. Il est tout aussi important d'effectuer des évaluations algorithmiques des risques pour s'assurer que les recommandations formulées ne reflètent pas des partis pris. L'intégration de l'IA aux services de sécurité des frontières possède le potentiel d'offrir une cohérence plus grande que celle qu'un être humain peut fournir. Il est essentiel de s'assurer que l'agent humain reste celui qui prend la décision et remet les analyses et les renseignements dans leur contexte en faisant appel à une intelligence émotionnelle qu'une machine n'a pas.

Il est essentiel de s'assurer que l'agent humain reste celui qui prend la décision et remet les analyses et les renseignements dans leur contexte en faisant appel à une intelligence émotionnelle qu'une machine n'a pas.

Les possibilités qu'offre l'IA pour la sécurité des frontières

Identification des voyageurs et exactitude
Utilisation de l'IA pour déceler dans les données des voyageurs des modèles de comportement qui pourraient indiquer des activités suspectes ou signaler qu'un agent doit procéder à un examen. Recours à la technologie biométrique pour assurer la concordance exacte entre un voyageur et ses documents de voyage et ainsi améliorer la circulation aux postes de contrôle de sécurité et ne désigner que certaines personnes dont le dossier semble présenter des irrégularités[13].

Surveillance et intégrité
Combinaison des données sur les tendances migratoires, les populations et l'environnement aux données sur l'activité aux frontières pour obtenir une meilleure compréhension de la situation aux postes frontaliers, se préparer en conséquence et déployer des agents de sécurité. Utilisation de capteurs intelligents et de la reconnaissance d'images pour améliorer les activités de surveillance et la détection des objets dans de grandes zones transfrontalières et pour que les agents de sécurité puissent réagir aux traversées non autorisées et à d'autres violations de la sécurité, plutôt que de faire des patrouilles ponctuelles[14].

Données et vision claire de l'objectif
Analyse des tendances dans les données sur les déplacements de grande envergure pour mieux affecter les ressources de sécurité[15]. Modélisation des effets des changements législatifs, comme la modification des politiques sur l'immigration. Utilisation de systèmes d'IA pour traiter les demandes d'immigration en ligne et réduire le nombre de tâches manuelles.

Douanes et confiance
Utilisation de la vision par ordinateur pour mieux analyser les images produites par rayon X des cargaisons et des bagages et repérer les marchandises dangereuses. Analyse des métadonnées sur les expéditions pour suivre et déceler les cas de contrebande et d'autres activités illicites.

Douaniers et vitesse d'exécution

Aux postes frontaliers, les contrôles peuvent être fastidieux autant pour les douaniers que pour les conducteurs de camion de fret. Les fouilles et les inspections manuelles prennent du temps. À l'aide des technologies de reconnaissance des visages et des images, le visage du conducteur et la plaque d'immatriculation de son véhicule pourraient être numérisés et examinés avant que le conducteur ne se présente aux douanes, ce qui permettrait d'accélérer le processus et de repérer les conducteurs auxquels un douanier doit poser d'autres questions. Une technologie de détection à rayon X améliorée par l'IA pourrait permettre de repérer avec exactitude et en toute sécurité des marchandises potentiellement dangereuses ou des cargaisons anormales qui pourraient cacher des cas de contrebande.

Enfin, les systèmes d'IA peuvent rapidement analyser des métadonnées pour détecter des marchandises suspectes qui doivent être inspectées. L'IA facilite le rôle des douaniers en leur donnant accès à des renseignements exacts en temps voulu.

Étendre l'utilisation de l'IA pour assurer la réussite à long terme du secteur de la défense et de la sécurité

Plus la *convergence* est forte entre l'être humain et la machine au sein d'une équipe, plus cette dernière est performante.

Pour intégrer les technologies d'IA à une organisation, il faut faire plus que simplement s'assurer que la technologie est fiable et sécuritaire; il faut aussi une stratégie favorisant l'adoption généralisée de l'IA, des processus pour obtenir et gérer les solutions, des données qui ne comportent pas de parti pris et des gens prêts à entretenir et à développer les capacités de l'IA. Les gouvernements adoptent de plus en plus un état d'esprit qui met le numérique au premier plan. Mais pour que le changement produise les résultats auxquels s'attendent les dirigeants, un changement de culture doit se faire au sein de la main-d'œuvre.

Quand ils disposent de la stratégie de gestion du changement appropriée, les organismes gouvernementaux, dont les forces armées, les services de police et les organisations assurant la sécurité des frontières, peuvent institutionnaliser des solutions d'IA régies avec un degré élevé d'imputabilité, facilement explicables et garantes de succès. La souplesse du processus d'approvisionnement permet aux équipes de commencer par mettre en place de petits projets pilotes pour tester les solutions et profiter d'occasions d'intégration et de formation, éléments clés de la convergence entre l'être humain et l'IA.

Lorsque les projets pilotes donnent des résultats positifs, les solutions peuvent être mises en place à l'extérieur des cas d'utilisation prévus à l'origine, ce qui élargit la portée de la solution et produit un effet sur d'autres aspects de l'organisation. Tout au long de ce processus, rien n'est plus important que l'intervention humaine à tous les stades de la mise en œuvre.

Adoption généralisée pour une réussite à long terme

L'adoption de l'IA au sein d'une organisation exige une vision stratégique de l'utilisation qui en sera faite et de sa mise en œuvre. Pour que les solutions mises en place donnent des résultats concrets et continus, il faut une vision plus large de ce que l'IA pourra accomplir. En établissant les bases du rôle de l'IA, l'organisation peut aller de l'avant avec des solutions qui permettront de réaliser sa vision et réutiliser des modèles testés pour diverses applications dans différents services, lorsqu'il est judicieux de le faire.

Stratégie
Élaborer une stratégie pour s'assurer que l'IA est largement adoptée et procure un succès mesurable à l'organisation.

Processus
Mettre en place des processus pour se procurer des solutions et régir l'utilisation éthique de l'IA.

Technologie
Acheter des solutions technologiques fiables et sécuritaires.

Données
Utiliser des données qui ne comportent pas de parti pris et peuvent être utilisées pour entraîner des algorithmes.

Gens
Donner au personnel le pouvoir d'entretenir et de développer les capacités de l'IA.

Demain : s'assurer que l'être humain fait partie du cycle

L'IA offre une occasion incroyable d'améliorer et d'intensifier notre façon de travailler.

La notion d'automatisation intelligente a suscité de l'inquiétude chez de nombreuses personnes quant à la sécurité d'emploi, mais en fait la technologie ne remplacera pas complètement l'être humain, elle ne l'a d'ailleurs jamais fait. Les technologies d'IA remplaceront certaines tâches précises, ce qui donnera aux travailleurs le temps et l'énergie d'entreprendre des tâches plus complexes fondées sur le raisonnement qui exigent quelque chose que l'IA ne possède pas : l'intelligence émotionnelle[16]. L'un des plus grands avantages de l'IA est sa capacité à effectuer des analyses de tendances complexes que l'être humain ne peut pas faire en raison du volume de données à traiter. Dans le secteur de la défense et de la sécurité, cette capacité permet aux responsables de protéger nos pays et nos collectivités et d'obtenir des renseignements critiques qui les aident à remplir leur mission plus efficacement. Les opérations et les interférences humaines sont extrêmement préoccupantes dans le secteur de la défense et de la sécurité, car le risque est plus grand. Le recours à l'IA exige davantage d'imputabilité et de fiabilité que dans d'autres secteurs, car des vies, du matériel coûteux et la sécurité des citoyens sont en jeu. Les responsables doivent être en mesure d'expliquer pourquoi et comment un modèle ou un algorithme est arrivé à un résultat particulier, et prendre la décision définitive. L'IA ne doit pas remplacer une décision humaine, elle sert plutôt à réaffecter les ressources à des activités de plus grande valeur. La conception des solutions d'IA doit dès le départ avoir comme priorité l'être humain et la confidentialité, ce qui les protège contre de graves conséquences.

Les gouvernements sont prêts à prendre des mesures immédiates de mise en œuvre de l'IA qui pourraient changer considérablement les flux de travaux et les résultats. Les technologies de l'IA peuvent servir à optimiser et à protéger les actifs, à augmenter les ressources, à améliorer la collecte et l'interprétation des données et à réduire les coûts, en fait à changer le secteur. Il est vraiment temps de passer à l'IA.

L'être humain fait partie du cycle

Données
L'opérateur humain choisit des données sans parti pris; l'IA trie et classe les données.

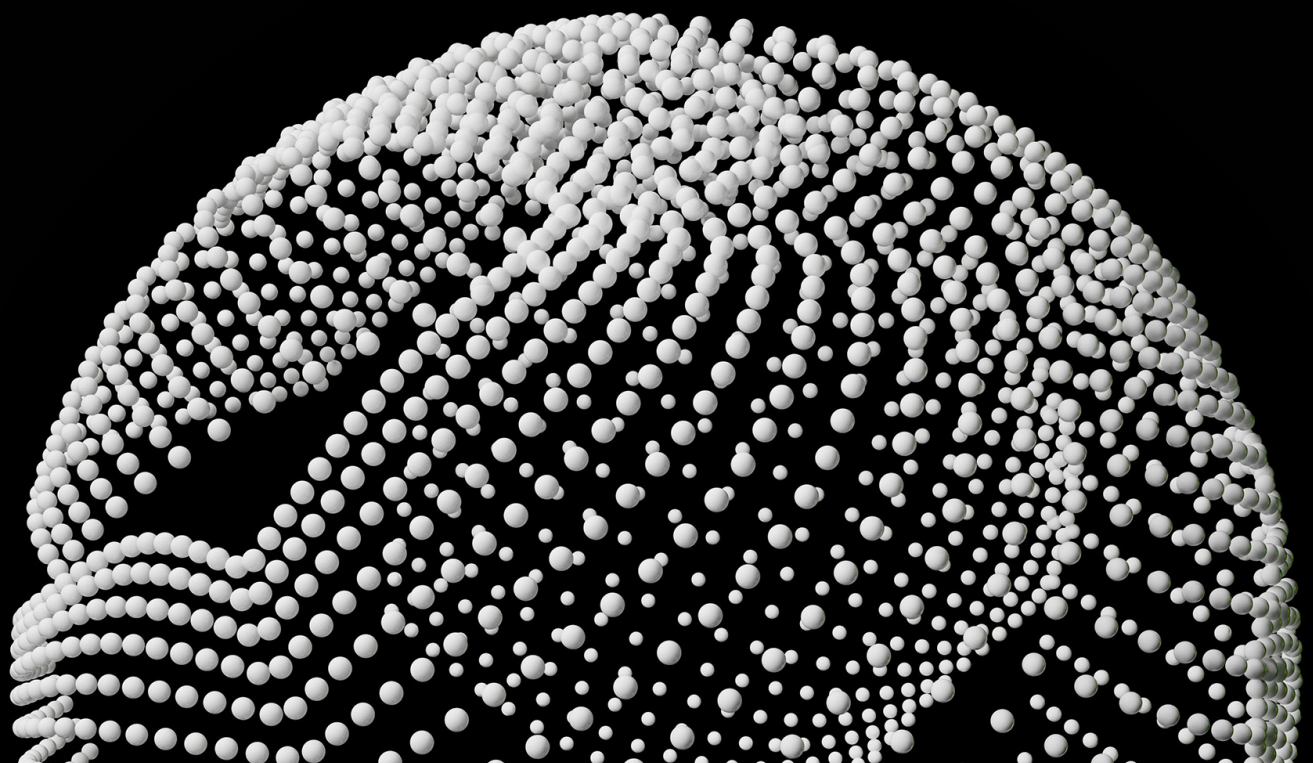
Perspectives
L'IA trouve les tendances et les données aberrantes en utilisant le processus le plus efficient et les soumet à l'examen de l'opérateur humain.

Inférences
L'IA formule des suggestions en fonction de règles définies par l'opérateur humain.

Jugement
L'opérateur humain détermine la meilleure marche à suivre en fonction du contexte.

Action
L'opérateur humain applique la décision ou indique à l'IA de le faire.

Examen approfondi sous la perspective de l'IA



La vision par ordinateur au service de la sécurité des frontières

Précision et efficacité accrues de la détection à rayon X

L'interprétation des images à l'écran monopolise une importante main-d'œuvre. Les agents affectés à la sécurité des frontières inspectent pendant de longues heures les écrans des appareils de détection, à l'affût de toute image de marchandises dangereuses contenues dans les colis et le fret. Après un certain temps de cette tâche laborieuse, rien d'étonnant à ce que certains articles échappent à leur vigilance ou s'avèrent difficiles à interpréter. L'IA pourrait venir à leur rescousse.

Faisant appel à des technologies de reconnaissance d'images de pointe, l'IA donne aux agents de sécurité la capacité de détecter les marchandises dangereuses avec plus d'acuité. Reposant à la fois sur des bibliothèques à source ouverte et sur l'infrastructure infonuagique, les algorithmes de vision par ordinateur peuvent être entraînés à détecter des objets particuliers – comme des armes à feu ou des explosifs – parmi d'autres images en arrière-plan, ce qui accroît l'exactitude des détections tout en diminuant le nombre de fausses alertes.

Voici quelques-uns de ces modèles :

YOLO : détection d'objets en temps réel

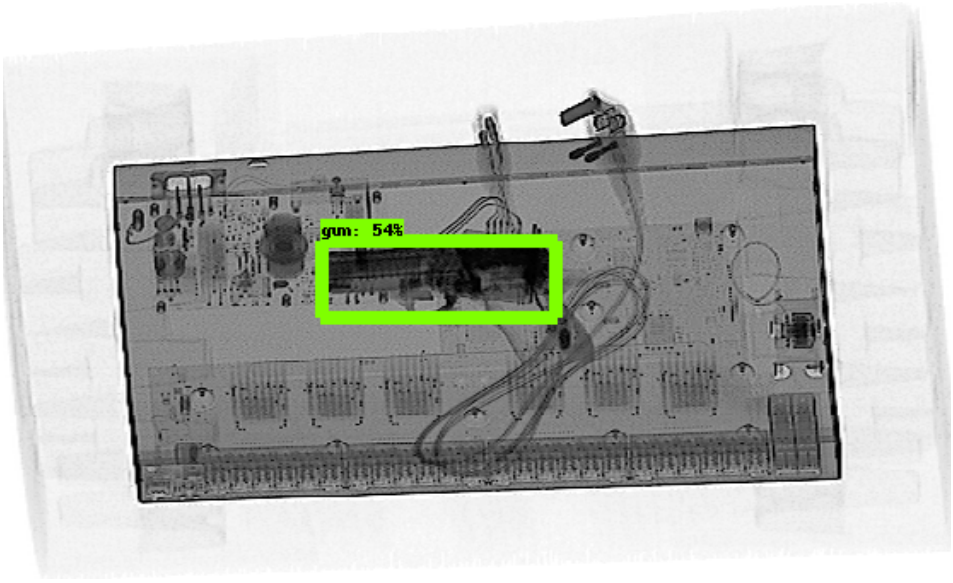
- Un réseau neuronal unique est appliqué à toute l'image et la divise en aires.
- Des zones de délimitation et des probabilités sont calculées pour chaque aire, les zones étant pondérées par les probabilités calculées, puis une certaine valeur est appliquée aux détections et seules les détections obtenant un pointage élevé sont montrées à l'utilisateur.

SSD : détecteur à photo unique

- Un réseau neuronal profond unique combine la division en aires et l'extraction des éléments de l'image.
- Différentes prédictions de zones de délimitation sont produites par chacune des dernières couches du réseau à l'origine des prédictions; on obtient des zones de délimitation de plus en plus petites, et la prédiction finale correspond à un amalgame de toutes ces prédictions.

RetinaNet

- Il s'agit d'un détecteur à phase unique (p. ex. YOLO ou SSD) doté de la performance des détecteurs à deux phases (p. ex. Faster-RCNN).
- Dans un réseau à pyramide d'images de type FPN, la perte d'entropie croisée est remplacée par la perte de focale.



La cybersécurité à l'échelle de l'organisation

L'IA contre les cybermenaces

Les professionnels des TI et de la sécurité des services gouvernementaux doivent protéger leurs actifs, assurer la sécurité des données sensibles et prémunir l'organisation contre toute atteinte à sa sécurité. Les directeurs des opérations de sécurité, par exemple, ont besoin de rapports en temps réel pour s'acquitter de leurs tâches. Quant aux administrateurs des TI, ils doivent savoir quels actifs sont les plus exposés et quels domaines doivent être protégés en priorité. Les analystes de la sécurité, enfin, pourraient mieux faire leur travail s'ils disposaient d'analyses par simulation pour prédire et prévenir les cyberattaques et activer des fonctions de contrôle de la sécurité.

Une plateforme intégrée globale permet à divers membres du personnel des TI d'avoir une meilleure vision de l'état de la cybersécurité; elle peut même formuler des recommandations sur les correctifs à apporter avant que les attaques surviennent.

En analysant la connectivité et la vulnérabilité des actifs ainsi que les risques auxquels sont exposés les actifs d'importance critique, cette solution d'IA peut illustrer l'état actuel de la cybersécurité et repérer le chemin qui offrirait le moins de résistance à une éventuelle attaque extérieure. Les données d'entrée comprennent l'architecture de réseau et de sécurité, la base de gestion de la configuration, les points de sortie et les journaux d'accès, les journaux des systèmes SIEM et les résultats des évaluations du risque.

L'analyse des données, combinée à la puissance d'algorithmes d'apprentissage machine de pointe, peut établir des recoupements entre les scénarios des cybermenaces, les signatures des attaques et les vulnérabilités pour alimenter un moteur de recommandations qui propose plusieurs mesures correctives possibles et fait en sorte que les nouvelles menaces soient signalées en temps quasi réel.

Signalement des menaces en temps quasi réel par le recoupement des scénarios des cybermenaces, des signatures des attaques et des vulnérabilités.

Outiller les fonctions de soutien

Gestion de l'approvisionnement et des fournisseurs

Dans les organismes gouvernementaux complexes, qui comportent plusieurs divisions, il est parfois très difficile de gérer les contrats, d'autant que l'évolution de la réglementation, les avancées rapides de la technologie et les pressions financières grandissantes forcent les ministères à faire toujours plus avec moins de ressources. Dans le secteur de la défense et de la sécurité, les contrats sont conclus à long terme; ils sont très confidentiels et très complexes.

En utilisant une solution de gestion des contrats fondée sur l'IA, les responsables de l'approvisionnement et des achats peuvent avoir une vision plus claire des groupes de contrats, des fournisseurs et des cycles d'approvisionnement. Grâce à la reconnaissance optique de caractères, les contrats papier peuvent être numérisés et passés en revue; la solution peut aussi aider à la préparation de la première ébauche standard d'un document. Toutes les négociations pourraient aussi avoir lieu dans le même système, l'IA signalant tout changement apporté à un contrat qui outrepasse la tolérance au risque de l'organisation.

Une fois le traitement effectué, le responsable des achats a une vue d'ensemble de tous les contrats conclus avec des fournisseurs, ce qui lui permet d'analyser les données recueillies. Il pourrait ainsi obtenir des renseignements sur la gestion des fournisseurs et savoir avec quels fournisseurs les négociations sont les plus longues, quelles dispositions sont le plus souvent révisées (ce qui pourrait indiquer que la première ébauche standard du contrat devrait être mise à jour) et combien de temps prend la réalisation complète de divers types de contrats d'approvisionnement, ce qui rendrait la planification plus efficace.

Automatisation et robots conversationnels intelligents

Les fonctions de soutien englobent les employés des services des finances et des ressources humaines qui effectuent des tâches administratives. Ces domaines comportent de nombreuses occasions d'intégrer l'IA de façon à réduire le nombre d'activités non essentielles qui prennent beaucoup de temps, ce qui permettrait aux employés de consacrer davantage de temps à des tâches dont la valeur est plus grande et qui font appel au jugement et au raisonnement humains.

Le robot conversationnel intelligent est l'une des solutions les plus faciles à mettre en œuvre. Avec l'aide d'un service automatisé, un robot conversationnel muni d'une fonction de traitement du langage naturel pourrait en effet répondre à des centaines de demandes que le service des RH reçoit chaque jour. Un robot conversationnel pourrait être mis en place dès le début du cycle de recrutement et répondre aux questions des candidats sur l'organisation et aussi recueillir les commentaires de ceux qui abandonnent leur démarche. Pour les employés, nouveaux ou actuels, un robot conversationnel intelligent peut répondre aux questions souvent posées sur l'intégration, la formation, la paie ainsi que sur les prestations de soins de santé, la couverture d'assurance et d'autres politiques.

Selon une analyse effectuée par Deloitte, au moins 21 % des heures de travail des employés fédéraux aux États-Unis sont consacrées à des tâches non essentielles, que les travailleurs jugent non importantes pour leur fonction. Il s'agit entre autres des activités de documentation et d'accès à l'information. Un robot conversationnel intelligent peut répondre aux demandes de renseignements, tandis que l'automatisation intelligente permet d'accélérer la saisie manuelle des données, la paperasserie, le suivi de l'information et l'établissement d'échéancier ainsi que de réduire le nombre de tâches en retard.

Maintenance prévisionnelle des actifs

Prévoir les défaillances avant qu'elles ne surviennent

La maintenance des actifs, parfois coûteuse, peut avoir de graves répercussions sur les missions et les opérations courantes lorsque des pannes imprévues surviennent. L'intégration de l'IA permet de fournir de l'information prédictive critique et d'éviter les perturbations opérationnelles et les temps d'arrêt inutiles touchant le matériel et d'autres types d'actifs.

En combinant les capteurs déjà installés sur certains actifs, comme les véhicules, et un logiciel d'IA, le système peut repérer les pièces qui doivent être réparées avant qu'elles ne cessent de fonctionner. Les renseignements physiques sur l'actif sont convertis en un format numérique que la machine peut analyser. Cette technologie fait appel à l'apprentissage machine pour analyser la grande quantité de données disponibles en temps réel et fournir des renseignements sur la probabilité de défaillance d'une pièce ou sa durée de vie. Grâce à la collecte d'un nombre toujours plus imposant de données au fil du temps, des renseignements de plus en plus utiles peuvent être générés pour établir des liens entre des événements qui pourraient entraîner des défaillances, et faire en sorte que d'autres actifs similaires soient améliorés avant une grave panne et que le matériel désuet soit remplacé par des outils plus efficaces.
De plus, la création d'un réseau branché de pièces d'équipement ou de composantes d'actifs produit des données de plus grande envergure qui permettent des analyses plus précises. Cette vue complète des composantes assure une plus grande transparence du processus décisionnel stratégique et l'optimisation de la performance.

L'intégration de l'IA à la maintenance des actifs et du matériel permet d'obtenir des renseignements utiles se traduisant par des stratégies de maintenance plus efficaces, l'optimisation des ressources et la réduction des dépenses globales consacrées aux activités de réparation.

Analyse de grandes quantités de données sur les actifs et génération de renseignements pour l'élaboration de stratégies de maintenance des actifs plus efficaces et efficientes.

Photo: Defense Dept.


HUMAIN
HUMAIN
HUMAIN

Notes de fin

1. « Military readiness through AI », Deloitte Insights, https://www2.deloitte.com/insights/us/en/industry/public-sector/ai-military-readiness.html (consulté le 9 mai 2019).
2. « In New Military, Data Overload Can Be Deadly », The New York Times, https://www.nytimes.com/2011/01/17/technology/17brain.html (consulté le 9 mai 2019).
3. « Artificial intelligence – what implications for EU security and defence? », Institut d'études de sécurité de l'Union européenne, https://www.iss.europa.eu/content/artificial-intelligence-%E2%80%93-what-implications-eu-security-and-defence (consulté le 31 mai 2019).
4. Lindsey R. Sheppard, « Artificial Intelligence and National Security; The Importance of the AI Ecosystem », Center for Strategic & International Studies: p. 21, https://www.csis.org/analysis/artificial-intelligence-and-national-security-importance-ai-ecosystem (consulté sur Internet le 31 mai 2019).
5. « 8 Key Military Applications for Artificial Intelligence in 2018 », Market Research.com, https://blog.marketresearch.com/8-key-military-applications-for-artificial-intelligence-in-2018 (consulté le 31 mai 2019).
6. « Today's battle for the electromagnetic spectrum », Military & Aerospace Electronics, https://www.militaryaerospace.com/communications/article/16709112/todays-battle-for-the-electromagnetic-spectrum (consulté le 31 mai 2019).
7. « AI Puts Army's Electronic Warfare Missions in Focus », MeriTalk, https://www.meritalk.com/articles/ai-puts-armys-electronic-warfare-missions-in-focus/ (consulté le 31 mai 2019).
8. Règlement (UE) général sur la protection des données (RGPD), paragraphe 71 du préambule, http://www.privacy-regulation.eu/fr/r71.htm (consulté le 31 mai 2019).
9. « How AI will transform digital evidence management », PoliceOne.com, https://www.policeone.com/police-products/body-cameras/articles/476484006-How-AI-will-transform-digital-evidence- management/ (consulté le 31 mai 2019).
10. « The border guards you can't win over with a smile », BBC, https://www.bbc.com/future/article/20190416-the-ai-border-guards-you-cant-reason-with (consulté le 31 mai 2019).
11. « Why More Border Patrol Agents Quit », AFGE, https://www.afge.org/article/why-more-border-patrol-agents-quit/ (consulté le 31 mai 2019).
12. « Artificial Intelligence Helps Keep Borders Safe », iHLS, https://i-hls.com/archives/88465 (consulté le 31 mai 2019).
13. « L'Intelligence Artificielle au service de la maîtrise des frontières », IDEMIA, https://www.idemia.com/fr/actualite/lintelligence-artificielle-au-service-de-la-maitrise-des-frontieres-2018-11-16 (consulté le 31 mai 2019).
14. Lindsey R. Sheppard, « Artificial Intelligence and National Security; The Importance of the AI Ecosystem », Center for Strategic & International Studies: p. 11, https://www.csis.org/analysis/artificial-intelligence-and-national-security-importance-ai-ecosystem (consulté le 31 mai 2019).
15. « Artificial Intelligence Helps Keep Borders Safe », iHLS.
16. « The border guards you can't win over with a smile », BBC.

Personnes-ressources

Leaders sectoriels

Beth McGrath
Leader, Défense, sécurité et justice
Deloitte mondial
bmcgrath@deloitte.com

Ed Delaney
Leader spécialiste, Capital humain
Deloitte États-Unis
edelaney@deloitte.com

Scott Savage
Leader, Transformation du secteur public
Deloitte Canada
scsavage@deloitte.ca

Leaders de l'IA à l'échelle mondiale

Jas Jaaj
Associé, Omnia IA
Deloitte Canada
jjaaj@deloitte.ca

Shelby Austin
Associée directrice, Omnia IA
Deloitte Canada
shaustin@deloitte.ca

Costi Perricos
Consultation
Deloitte Royaume-Uni
cperricos@deloitte.co.uk

Nitin Mittal
Associé, Services d'analytique
Deloitte États-Unis
nmittal@deloitte.com

Collaborateurs

Nihar Dalmia
Leader, Omnia IA,
Services gouvernementaux et publics
Deloitte Canada
nidalmia@deloitte.ca

Andrew McHardy
Directeur principal, Omnia IA
Deloitte Canada
amchardy@deloitte.ca

Bilal Jaffery
Directeur principal, Omnia IA
Deloitte Canada
bjaffery@deloitte.ca

Jana Betik
Conseillère principale, Omnia IA
Deloitte Canada
janabetik@deloitte.ca

L’ère de la *convergence*

Explorez notre série sur Deloitte.ca

L’ère de la *convergence*
Tirer parti de l’IA pour créer l’entreprise de détail de l’avenir

L’ère de la *convergence*
Assurance : pour accélérer le déploiement de l’intelligence augmentée

L’ère de la *convergence*
L’avenir du secteur Énergie, ressources et produits industriels dans le contexte de l’IA

Deloitte.

Deloitte offre des services dans les domaines de l’audit, de la certification, de la consultation, des conseils financiers, des conseils en gestion des risques et de la fiscalité, et des services connexes, à de nombreuses entreprises du secteur privé et public. Deloitte sert quatre entreprises sur cinq du palmarès Fortune Global 500® par l’intermédiaire de son réseau mondial de cabinets membres dans plus de 150 pays et territoires, qui offre les compétences, le savoir et les services de renommée mondiale dont les clients ont besoin pour surmonter les défis d’entreprise les plus complexes. Pour en apprendre davantage sur la façon dont les quelque 264 000 professionnels de Deloitte, dont 14 000 au Canada, ont une influence marquante, veuillez nous suivre sur LinkedIn, Twitter ou Facebook.

Deloitte désigne une ou plusieurs entités parmi Deloitte Touche Tohmatsu Limited, société fermée à responsabilité limitée par garanties du Royaume-Uni, ainsi que son réseau de cabinets membres dont chacun constitue une entité juridique distincte et indépendante. Pour obtenir une description détaillée de la structure juridique de Deloitte Touche Tohmatsu Limited et de ses sociétés membres, voir www.deloitte.com/ca/apropos.

© 2019 Deloitte S.E.N.C.R.L./s.r.l. et ses sociétés affiliées.

Conçu et produit par le Service de conception graphique de Deloitte, Canada. 19-6498H