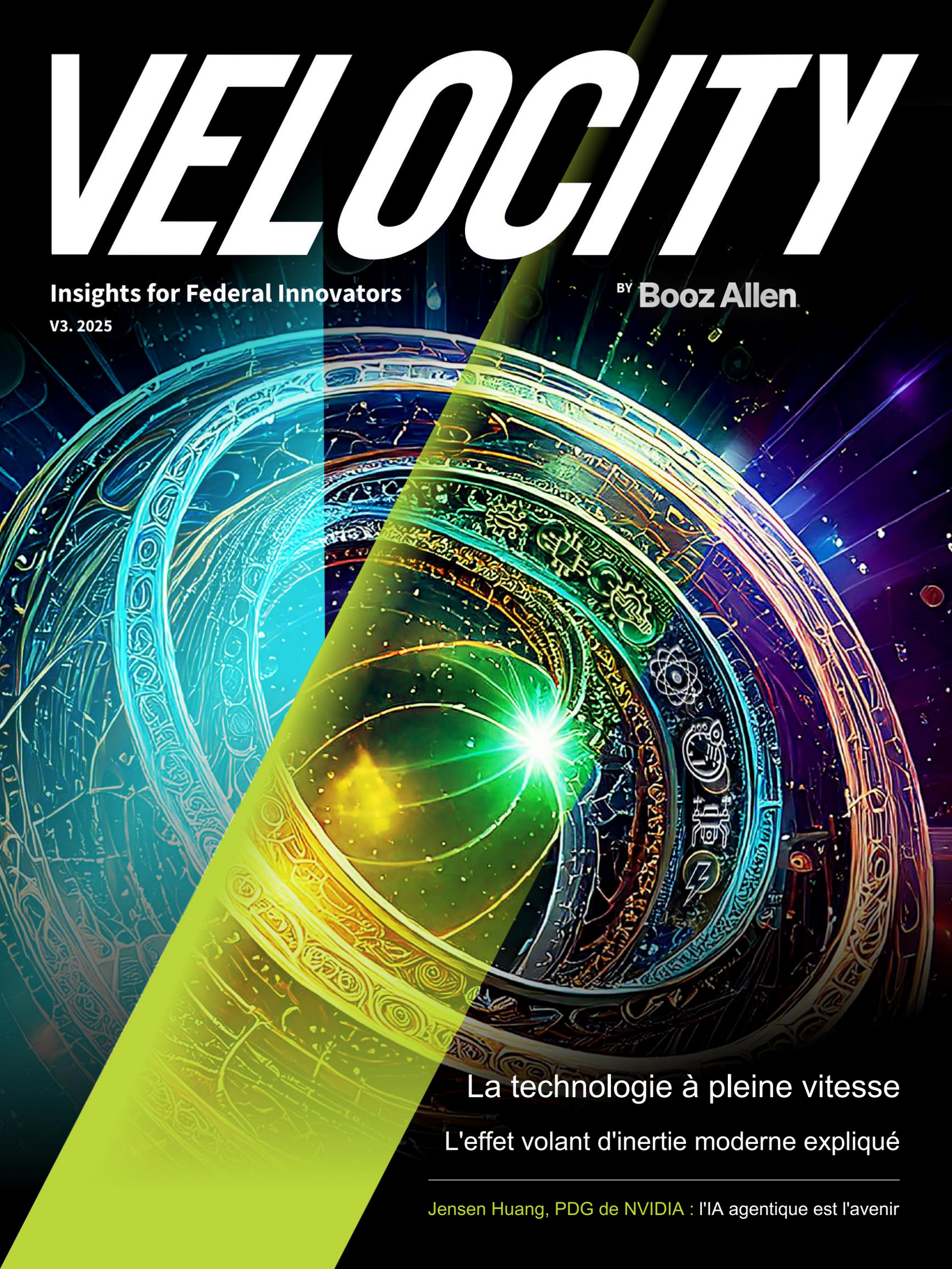
VELOCITY

Insights for Federal Innovators

V3. 2025

BY Booz Allen



La technologie à pleine vitesse

L'effet volant d'inertie moderne expliqué

Jensen Huang, PDG de NVIDIA : l'IA agentique est l'avenir

À PROPOS DE LA

COUVERTURE : La couverture a été conçue par Brody Rose. Elle utilise des images générées par l'IA d'Adobe Firefly pour représenter la convergence des technologies émergentes vers un système intelligent et auto-optimisé.

NOTE AUX LECTEURS

Les idées et opinions présentées ici sont celles de leurs auteurs respectifs. Elles constituent des réflexions dans les domaines techniques abordés. Elles ne représentent pas nécessairement le point de vue du cabinet, mais reflètent l'étendue, la profondeur et l'actualité du talent technique de Booz Allen et de ses associés.

Les références à des produits ou à des entreprises ne constituent pas une approbation de Booz Allen ou de tout autre contributeur.

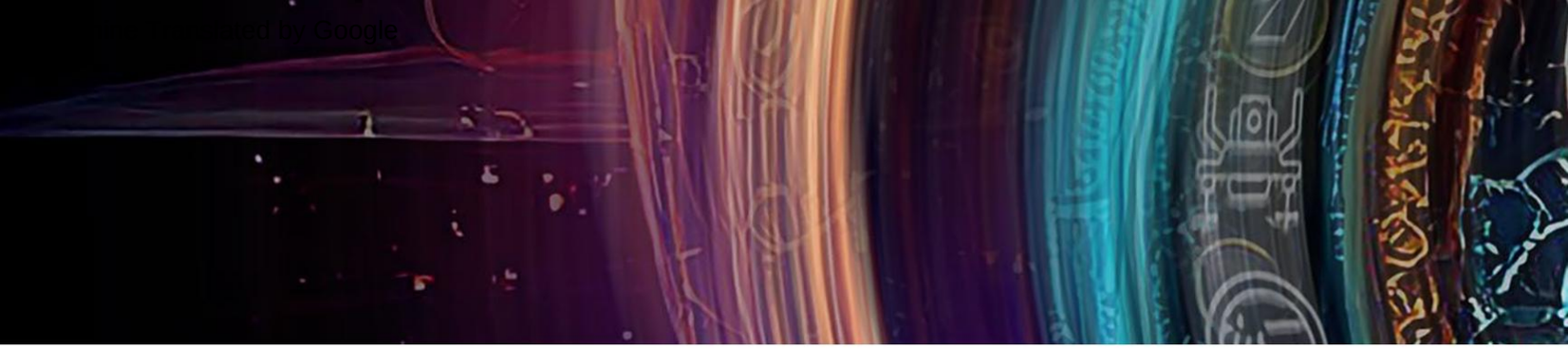
Contenu

DÉPARTEMENTS

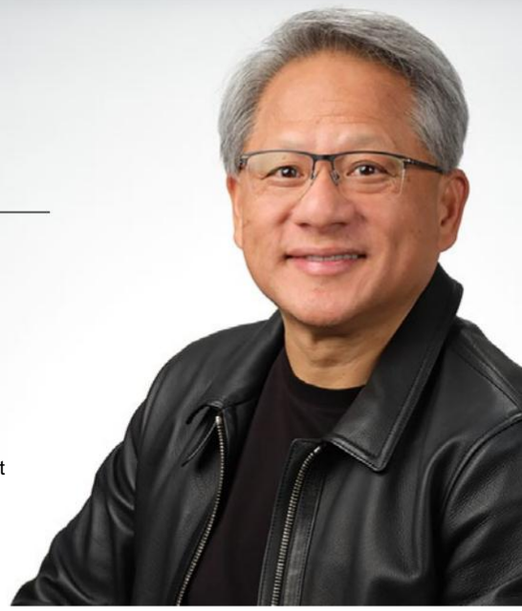
« Les agences fédérales ont le « Une opportunité unique de définir la norme pour l'IA opérant dans des environnements à haut risque. La prochaine étape consistera à faire évoluer l'IA pour prendre des décisions plus rapides et plus précises, tout en garantissant la transparence, la sécurité et la fiabilité de ces systèmes

– Jensen Huang, fondateur et PDG de NVIDIA

Digitized by Google



CARACTÉRISTIQUES



POINTS FORTS DE LA MISSION

Machine Translated by Google

TECHNOLOGIES ÉMERGENTES

Machine Translated by Google

Booz Allen a commémoré son 110e anniversaire
anniversaire à la Bourse de New York

Machine Translated by Google

DU DIRECTEUR DE LA TECHNOLOGIE

Missions et résultats concrets ? Telle est la question essentielle à laquelle notre nation est confrontée alors que nous entrons dans une nouvelle ère caractérisée par des avancées technologiques rapides.

Comment pouvons-nous exploiter les technologies commerciales les plus avancées pour accélérer le processus fédéral ? Aujourd'hui, les entreprises du secteur privé élargissent le champ des possibles dans des domaines tels que l'intelligence artificielle (IA), le cloud computing, les jumeaux numériques, etc. Parallèlement, notre pays est confronté à un environnement de sécurité nationale des plus complexes depuis l'apogée de la Guerre froide, tandis que la pression croissante d'une dette publique insoutenable menace la croissance économique nationale. Dans ce contexte de défis complexes, il est clair que la rapidité d'innovation n'est plus un avantage stratégique, mais un impératif.

Dans ce numéro de Velocity, nous examinons l'évolution de la technologie et ses applications pour accélérer l'innovation, améliorer l'efficacité et améliorer le bien-être des Américains. Depuis la publication de notre dernier numéro sur l'omniprésence de l'IA, l'idée d'une technologie en pleine expansion a pris une importance accrue. L'IA n'est pas seulement intégrée aux missions les plus critiques ; elle réinvente le rythme et les méthodes de développement et de déploiement de toutes les technologies (voir mon article de couverture sur l'effet volant d'inertie moderne, page 32). Par conséquent, nous sommes au bord de l'une des vagues technologiques les plus importantes de l'histoire.

En tant que principal fournisseur de solutions d'IA pour le gouvernement américain, nous avons la responsabilité de veiller à ce que les agences fédérales puissent utiliser l'IA et d'autres technologies émergentes pour moderniser leurs capacités actuelles, améliorer les performances humaines et construire les systèmes de demain. Il est temps de repenser la collaboration entre les secteurs public et privé (voir notre entretien avec Jensen Huang, PDG de NVIDIA, page 28). En abordant cette situation avec une approche axée sur les résultats et l'efficacité, nous pouvons tracer la voie vers un avenir plus résilient, plus sûr et plus prospère.

Alors que nous nous engageons à construire cet avenir ensemble, je vous invite à découvrir les points de vue et les perspectives des experts en technologie de Booz Allen et de l'ensemble du secteur. Le magazine de cette année aborde :

- Comment l'IA générative évolue des modèles uniques à grand langage vers des systèmes multi-agents (voir notre article sur l'IA agentique à la page 41)

- Pourquoi les systèmes terrestres virtuels joueront un rôle clé dans la protection des ressources spatiales américaines (voir notre focus sur les missions spatiales à la page 17)

- Le potentiel de l'IA pour réinventer la manière dont les équipes de cybersécurité mènent la chasse aux menaces (voir notre article sur la cybersécurité alimentée par l'IA à la page 11)

Depuis 11 décennies, Booz Allen est un pionnier de l'innovation pour ses clients. Notre expérience nous a appris que les périodes de grands changements peuvent engendrer les transformations les plus remarquables. Dans un monde où la technologie définit l'avenir, saisissons cette occasion pour révolutionner le monde.

Bill Vass

directeur de la technologie
Booz Allen

Réflexions sur l'IA générative

LEÇONS APPRISES DE DEUX ANNÉES D'INVITATION

Ernest Sohn et Alison Smith

L'attribut le plus remarquable de l'intelligence artificielle Générative (GenAI) est la rapidité avec laquelle il La technologie continue de progresser. Plus de deux ans après la sortie de ChatGPT, les capacités émergentes des premiers modèles pionniers comme GPT-3 – telles que les compétences en programmation informatique et les premiers signes de raisonnement – sont désormais au cœur des compétences des modèles plus récents et plus avancés. Un article publié sur Windows Central indique que les modèles o1 et o1-mini d'OpenAI ont démontré leur capacité à réussir l'entretien d'embauche d'ingénieur de recherche en codage de l'entreprise. En octobre 2024, Anthropic a annoncé qu'elle apprendrait à son assistant IA Claude à utiliser un ordinateur comme un humain et à s'attaquer à des tâches ouvertes comme la conduite de recherches.

Bien que les capacités technologiques de GenAI progressent à un rythme accéléré, son impact au niveau des entreprises est plus nuancé. En termes simples, la technologie n'a pas encore réalisé d'opérations complexes de manière cohérente et compétente sans intervention humaine.

Ce paradigme va probablement changer au cours des trois prochaines années à mesure que la technologie sous-jacente mûrit et que les entreprises associent de grands modèles linguistiques (LLM) et d'autres types de GenAI avec d'autres technologies et entre eux pour créer des systèmes intelligents avec des niveaux d'autonomie plus élevés.

Avec ces avancées à l'horizon, il est devenu plus facile de voir clairement GenAI, à la fois dans sa puissance créative et dans ses lacunes existantes. Chaque question répondue révèle une nouvelle vérité sur le fonctionnement interne de la technologie, et nous pouvons désormais tirer le bilan de ce que nous avons appris en plus de deux ans de questions. Voici quelques perspectives clés sur l'évolution de GenAI : du rôle inestimable que jouent les humains dans son déploiement aux implications de sa nature stochastique et aux types de cas d'utilisation pour lesquels il est le mieux adapté.

Les meilleurs cas d'utilisation de GenAI

Entre la confirmation de ses promesses et ses pannes parfois déroutantes, GenAI continue de se rapprocher du cœur des missions critiques. Dans le secteur manufacturier, la technologie modernise les processus clés, notamment les systèmes de réponse aux incidents qui exploitent des copilotes interactifs pour anticiper et résoudre proactivement les problèmes avec une intervention humaine minimale. Dans le cadre d'une initiative de la Defense Advanced Research Projects Agency, GenAI identifie désormais et corrige les vulnérabilités des logiciels open source sous-jacents aux infrastructures critiques.

La capacité d'innovation rapide de cette technologie lui confère le potentiel d'aider les agences à résoudre des problèmes d'importance nationale cruciale. Avant que ces transformations radicales ne se produisent, les agences peuvent tirer profit de l'un de ses cas d'utilisation les plus prolifiques et éprouvés : l'amélioration de l'efficacité opérationnelle. L'Office américain des brevets et des marques, par exemple, exploite ses puissantes capacités de recherche pour aider les examinateurs à trouver plus rapidement les documents pertinents lors du traitement des demandes de brevet. Le ministère de la Défense a développé l'outil de rédaction Acqbot afin de réduire le temps et les efforts humains nécessaires à la génération de contrats. Le point commun de ces applications est l'accent mis sur l'utilisation de GenAI pour aider les employés à accomplir leurs tâches quotidiennes plus efficacement. Cependant, ces types de projets ne représentent que des succès d'adoption précoce génériques, aux effets limités. Les cas d'utilisation matures du futur seront bien p impliquera de combiner GenAI avec d'autres types d'IA pour créer un impact maximal.

Aujourd'hui, les organisations peuvent utiliser GenAI pour opérationnaliser des applications allant des chatbots de service client et

Figure 1 : Différents types d'IA

IA traditionnelle	IA générative
Exactitude : Précision et fiabilité des résultats	Créativité : Invention de nouvelles idées et conclusions logiques
Interprétabilité : Accès aux décisions et aux résultats du modèle	Généralisabilité : application des connaissances acquises à des données nouvelles et invisibles

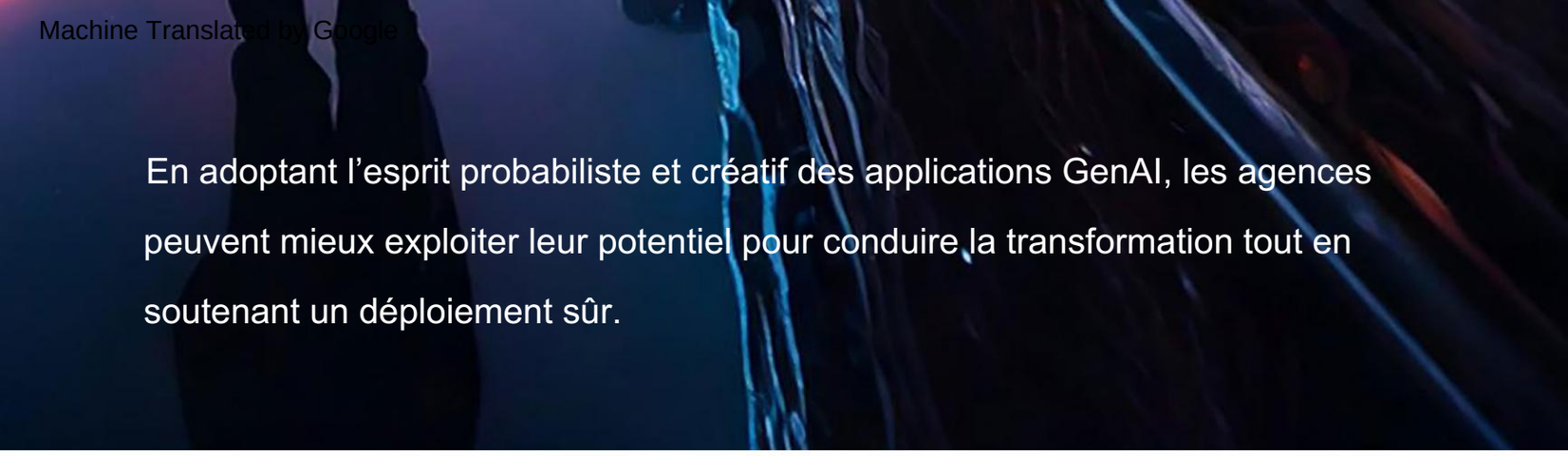
Machine Translated by Google

Des agents de codage logiciel aux outils de découverte scientifique et d'arbitrage politique, tous ces outils s'appuient sur la capacité de GenAI à exécuter rapidement et efficacement des fonctions humaines, telles que la recherche d'informations, l'agrégation de données, la synthèse, l'interprétation, le traitement analytique, la synthèse, la modélisation prédictive, la conception itérative et, bien sûr, la génération de contenu.

Néanmoins, GenAI n'est pas encore adapté à toutes les tâches. Les cas d'utilisation nécessitant des résultats plus précis, explicables et prévisibles, comme la fabrication de précision ou la surveillance de la sécurité des réseaux, pourraient être mieux traités par les algorithmes d'apprentissage automatique traditionnels. Pourquoi ? Contrairement aux algorithmes traditionnels, qui peuvent être développés pour produire le même résultat à partir des mêmes données d'entrée, les modèles GenAI peuvent générer des résultats différents grâce à leur utilisation de processus stochastiques. Les sources de variabilité tout au long du cycle de vie du modèle incluent, entre autres, les paramètres initialisés aléatoirement au sein des réseaux neuronaux et des techniques telles que l'échantillonnage de Monte-Carlo, qui introduit un caractère aléatoire dans le processus d'inférence. De plus, les algorithmes traditionnels d'apprentissage automatique sont hautement spécialisés en termes de données et de domaine, tandis que les modèles GenAI ont tendance à exceller dans leur généralisabilité.

La nature stochastique de l'IA Gen nécessite une analyse minutieuse des cas d'utilisation afin de calibrer avec précision les risques opérationnels et de mission. Pour des problèmes bien définis, avec des règles et des contraintes spécifiques, l'IA traditionnelle constitue souvent une option plus fiable, notamment lorsque l'utilisateur n'a pas besoin du modèle pour expliquer ses décisions. L'évaluation des compromis entre différents paradigmes d'IA permet aux agences d'identifier la bonne approche. En adoptant l'esprit probabiliste et créatif des applications de l'IA Gen, les agences peuvent mieux exploiter leur potentiel de transformation tout en garantissant un déploiement sécurisé.

Machine Translated by Google



En adoptant l'esprit probabiliste et créatif des applications GenAI, les agences peuvent mieux exploiter leur potentiel pour conduire la transformation tout en soutenant un déploiement sûr.

Comment soutenir une IA responsable ? Outre l'aide précieuse qu'ils apportent aux processus clés, les LLM ne peuvent ignorer leurs erreurs de calcul. Selon Tech Xplore

Dans un article publié en décembre 2023, des chercheurs de Google ont piégé ChatGPT en lui faisant divulguer des données d'entraînement sensibles lorsqu'on leur a demandé de répéter le mot « poème ».

Une étude publiée en décembre 2023 dans le Stanford Internet Observatory a indiqué que l'ensemble de données LAION-5B utilisé pour former Stable Diffusion contenait des centaines d'images illégales.

En effet, la croissance fulgurante de GenAI amplifie les inquiétudes concernant l'éthique, la sécurité et le développement responsable de l'IA. De ce fait, de nombreux pays ont exprimé leurs inquiétudes quant aux risques potentiels liés aux avancées de l'IA et ont plaidé en faveur d'une coopération internationale pour l'élaboration d'un cadre réglementaire commun.

Ces inquiétudes découlent du développement rapide de l'IA générative et de son impact considérable en tant que technologie polyvalente dans divers secteurs. En réponse, les nations ont commencé à former des alliances mondiales et à publier des déclarations visant à favoriser la collaboration et à établir des lignes directrices pour la gouvernance de l'IA. Parmi les exemples, citons le processus d'Hiroshima du G7 sur l'IA générative ; la déclaration de Bletchley affirmant l'engagement en faveur d'une IA sûre et centrée sur l'humain ; le Pacte numérique mondial des Nations Unies visant à créer un cadre éthique commun pour l'IA ; l'Alliance pour l'IA, pilotée par l'industrie ; et le Frontier Model Forum visant à promouvoir la recherche sur la sécurité de l'IA.

Bien que ces initiatives soulignent l'importance de la collaboration, une grande partie du langage employé dans ces déclarations reste vague et manque de suivi concret, ce qui soulève des questions quant à l'engagement réel en faveur de la gouvernance internationale. Il est également devenu évident que les pays, en particulier ceux qui ont un accès disproportionné aux ressources et aux capacités avancées en matière de production de puces et de modèles de base, peuvent donner la priorité à leurs intérêts nationaux.

Cette tendance suggère que, malgré l'apparence d'unité et de collaboration, de nombreux pays continuent de poursuivre des stratégies individuelles.

Bien que les efforts visant à codifier les approches d'une IA responsable aux niveaux national et mondial suscitent une nécessaire prise de conscience, ils ne devraient pas inciter les dirigeants à suspendre les initiatives GenAI en cours par crainte de dépasser certaines limites encore indéterminées. La meilleure voie à suivre consiste à concilier exploration et prudence en encourageant l'itération sur des cas d'utilisation à faible risque qui continueront de favoriser le développement et la compréhension sans repousser les limites de manière incontrôlée.

Rien ne remplace l'apprentissage par la pratique. C'est pourquoi la poursuite de la mise en production de GenAI permettra aux entreprises de réussir. Cela leur permettra également d'apporter de précieuses contributions au domaine de l'IA responsable, en développant une compréhension plus précise des garde-fous nécessaires pour concilier innovation et utilisation responsable.

Inciter avec un objectif et une expertise

Au cœur de cette expérimentation se trouve l'ingénierie des prompts, qui influence directement la qualité, la pertinence et la sécurité des résultats de l'IA. Si toute personne disposant d'une connexion internet peut utiliser les LLM commerciaux, il est indéniable que les utilisateurs expérimentés qui comprennent le fonctionnement de la technologie sous-jacente tireront une valeur significativement plus importante de GenAI. L'expertise en ingénierie des prompts permet au LLM de produire des résultats que les utilisateurs peuvent intégrer en toute confiance dans des bases de code, des bases de données et divers autres outils.

Composants d'un système. Une meilleure incitation produit un meilleur contenu.

L'importance de l'intuition humaine, associée à l'expertise du domaine, pour tirer profit des LLM explique pourquoi investir dans des programmes de formation visant à améliorer les compétences en IA, les compétences en ingénierie et les techniques de collaboration homme-machine des employés est l'un des meilleurs moyens pour les entreprises de garantir leur réussite. À mesure que le domaine de la collaboration homme-machine évolue, les personnes maîtrisant mieux le fonctionnement de l'IA et s'y adonnant seront les mieux placées pour intégrer cette technologie aux opérations de l'entreprise de la manière la plus efficace et responsable possible.

Le rôle essentiel de l'ingénierie des données

La réussite des applications GenAI d'entreprise nécessite la maîtrise de l'ingénierie rapide et de l'art et de la science de la préparation des données. Pourtant, nombreux sont ceux qui sous-estiment le rôle crucial de l'ingénierie des données dans l'orientation des LLM. Des fenêtres contextuelles volumineuses ne dispensent pas d'une préparation minutieuse des données ; le simple fait d'ajouter davantage de contenu brut à un LLM ne permet pas d'obtenir des résultats précis et fiables. Dans certains cas, ajouter trop de contexte introduit de nouveaux risques, comme la saturation de la capacité d'attention et la dilution des informations pertinentes. En particulier, les applications de génération augmentée de données (RAG) doivent se concentrer sur l'intégration efficace de données de haute qualité dans l'application LLM. Une préparation adéquate des données contribue au fonctionnement optimal des modèles, augmentant ainsi leurs chances de produire des résultats exploitables, précis et robustes, utilisables dans la prise de décision. À l'inverse, une préparation inadéquate ou insuffisante des données ouvre la voie à des hallucinations peu ou pas rentables pour les utilisateurs.

Machine Translated by Google

Les techniques traditionnelles de prétraitement des données restent tout aussi pertinentes pour les applications GenAI, notamment le nettoyage et le formatage de base, comme la suppression des informations personnelles identifiables (PII) ou des données non pertinentes ou incomplètes et la conversion des données restantes dans un format cohérent et la tokenisation, où le texte est divisé en unités plus petites et plus faciles à gérer.
De plus, des stratégies telles que l'optimisation du découpage, l'enrichissement des métadonnées, la recherche hiérarchique structurée et le reclassement contribuent à garantir que les systèmes RAG peuvent efficacement combler le fossé entre les informations brutes et les informations exploitables nécessaires aux cas d'utilisation et aux flux de travail spécifiques à l'entreprise. Par exemple, les approches de découpage par fenêtre glissante se sont avérées bien adaptées aux textes courts et moyens, où la continuité entre les segments est essentielle (par exemple, les conversations), tandis que les modèles hiérarchiques peuvent être adaptés au traitement de documents longs, nombreux et complexes.

Cet investissement initial dans la préparation des données, bien que gourmand en ressources, améliore en fin de compte la précision des réponses, réduit les coûts opérationnels et contribue à maintenir la conformité réglementaire tout en protégeant les informations sensibles grâce à un filtrage et des contrôles d'accès appropriés.

Quelle est la prochaine étape pour GenAI ?

Les progrès constants des capacités de GenAI incitent à spéculer sur les futurs apprentissages à distance. Cependant, toute prédiction sur l'avenir de cette technologie, axée exclusivement sur l'amélioration des performances des modèles, ignorerait plusieurs facteurs cruciaux et potentiellement atténuants.

Pour commencer, le coût de la formation des LLM monte en flèche et pourrait à terme devenir prohibitif. En août 2024, Epoch AI a publié un rapport précisant que, s'il est techniquement possible d'adapter la formation des modèles d'IA au rythme actuel, cela nécessitera des investissements de plusieurs centaines de milliards de dollars pour les développeurs au cours des prochaines années. Même si les coûts unitaires baissent, les coûts globaux élevés, conjugués à l'incertitude des coûts en aval, seront difficiles à accepter, même pour les entreprises technologiques les plus riches en liquidités, d'autant plus que les interrogations sur la capacité de la technologie à générer des rendements proportionnels se font de plus en plus vives.

À mesure que l'économie des modèles devient complexe à appréhender, le véritable coût de l'opérationnalisation de GenAI se déplacera de l'entraînement des modèles vers le point d'inférence, c'est-à-dire le déploiement de l'IA en environnement réel. Cela réorientera les discussions sur GenAI vers les meilleures pratiques d'ingénierie d'applications de bout en bout utilisant cette technologie pour des missions spécifiques, de la cybersécurité aux applications militaires en passant par les forces de l'ordre.

Les entreprises investiront davantage de temps et d'efforts dans la création d'ensembles d'évaluation permettant de comparer les applications d'IA aux indicateurs de performance traditionnels et de maîtriser les coûts. La manière dont les entreprises conçoivent leurs solutions déterminera en fin de compte leur capacité à utiliser GenAI pour créer de la valeur à des prix acceptables.

L'intégration verticale est une des solutions que les entreprises devront adopter pour s'adapter à cette nouvelle réalité. Les fournisseurs de matériel innovants au sein de la pile GenAI chercheront à créer des couches logicielles, tandis que les éditeurs de logiciels pourraient chercher à fabriquer leur propre matériel. Un bon exemple de cette intégration verticale est NVIDIA. L'entreprise, mondialement connue pour avoir conçu les processeurs graphiques à l'origine de la révolution de l'IA, s'appuie déjà sur son succès dans le domaine du matériel pour réinventer les capacités logicielles. NVIDIA a créé Omniverse, une plateforme permettant aux développeurs de simuler des mondes physiques avec une précision remarquable, et NIM Agent Blueprints, qui les aide à créer des applications utilisant un ou plusieurs agents d'IA.

Ces développements démontrent que la véritable puissance de GenAI va au-delà des remarquables capacités des algorithmes qui la sous-tendent. Comme toute révolution technologique, GenAI a démarré en fanfare. Vient maintenant une étape plus discrète, mais tout aussi percutante : son intégration aux applications de bout en bout, de manière rentable et innovante.

Ernest Sohn, responsable de l'IA au sein du bureau du directeur de la technologie de Booz Allen, fournit des services et des capacités d'IA pour aider les clients civils fédéraux à répondre aux besoins critiques de la mission.

Alison Smith, directrice de l'IA générative chez Booz Allen, dirige les solutions GenAI dans toute l'entreprise et aide les équipes à créer les meilleures pratiques pour le développement et l'utilisation de l'IA.

LECTURE RAPIDE

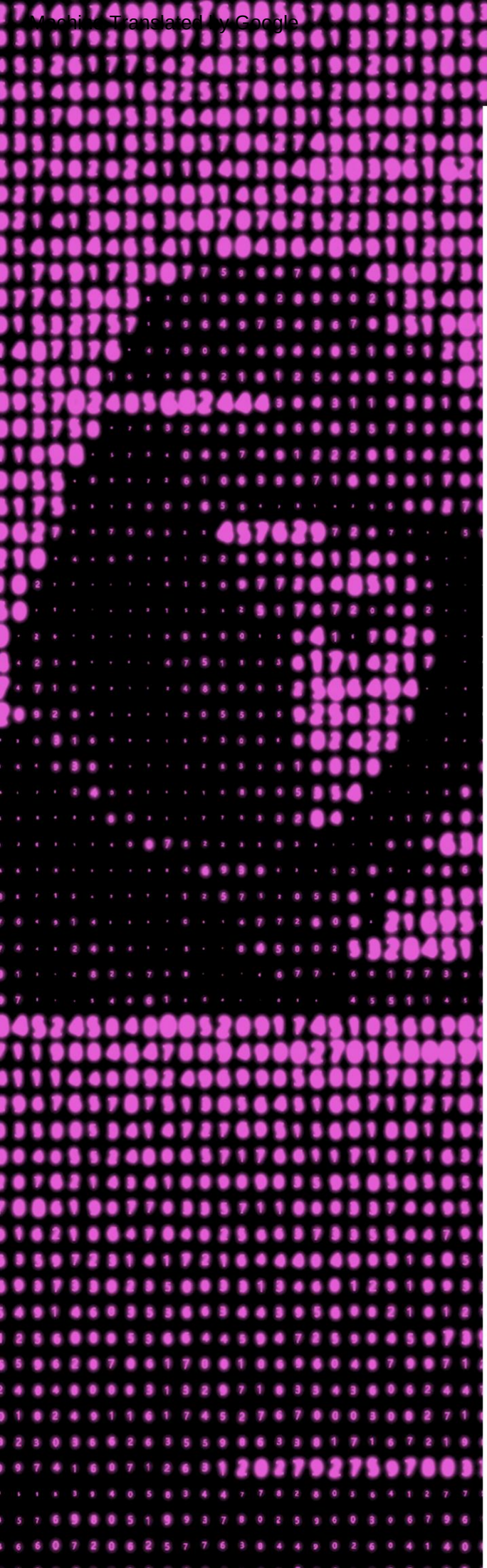
La superpuissance de l'IA générative réside dans la vitesse à laquelle elle progresse, un trait qui peut être observé dans la mesure où la technologie a progressé depuis le lancement de ChatGPT en novembre 2022.

Mais à mesure que le coût de formation des modèles à langage volumineux monte en flèche, les organisations se concentreront moins sur l'amélioration des performances des modèles et davantage sur l'opérationnalisation de la technologie au point d'inférence : là où l'IA est déployée dans des environnements réels.

À mesure que ce changement se produit, les organisations qui accordent la priorité à la maîtrise de l'IA et à l'ingénierie des données seront bien placées pour déployer l'IA générative de manière efficace et responsable.

Réaliser en temps réel Cyber Défense

Machine Translated by Google



Renforcer la cybersécurité Défenses avec IA

Tony Sharp, Joe Gillespie, Matt Costello, Mike Saxton et Rita Ismaylov

« C'était une réponse rapide et un confinement réussi », a déclaré le
Le responsable de la sécurité des systèmes d'information (RSSI) l'a déclaré. Mais ce n'était pas le cas.

Le centre des opérations de sécurité (SOC) a intercepté la première intrusion : une campagne d'e-mails de spear phishing soigneusement ciblée. Une cadre a transmis le message à l'équipe de sécurité, accompagné de son appât habilement conçu et d'une pièce jointe PDF malveillante. Elle leur a expliqué qu'il semblait provenir d'un contact de confiance, mais que l'adresse e-mail était inconnue.

Déclenché dans le sandbox du SOC, le malware s'est révélé et a tenté de se connecter à son infrastructure de commandement et de contrôle (C2). Armée de l'adresse C2, l'équipe a rapidement localisé la demi-douzaine d'autres e-mails malveillants dont les destinataires avaient ouvert la pièce jointe. Leurs appareils compromis ont été isolés et désinfectés.

Trois jours plus tard, l'équipe a bloqué la deuxième intrusion. Les attaquants ont utilisé des attaques par pulvérisation de mots de passe sur un portail de services cloud mal configuré. Leur script automatisé a tenté des centaines de connexions successivement avec des combinaisons d'adresses e-mail et de mots de passe récupérées lors de précédentes violations de données. Alerté par l'un de ses outils de sécurité des identités, le SOC a sécurisé le portail et mis à jour sa liste de blocage avec les adresses IP d'origine des tentatives de connexion.

Comme son homologue de nuit l'avait fait plus tôt pour l'attaque par spear-phishing, le responsable du SOC de jour a préparé un rapport répertoriant les tactiques, techniques et procédures (TTP) de l'attaquant ainsi que les indicateurs de compromission pertinents. Il a publié ce rapport anonymement via le centre d'analyse et de partage d'informations de son secteur afin d'alerter les autres entreprises de son secteur.

« Dans ces deux incidents », a insisté à juste titre le RSSI par la suite, « l'équipe a tout fait correctement. » Mais la troisième intrusion a tout de même été manquée.

La vulnérabilité fatale s'est avérée provenir d'un serveur web créé cinq ans plus tôt pour soutenir une série d'événements marketing d'entreprise, rapidement annulés et ratés. Il n'avait pas été mis à jour depuis des années, et les analyses menées par l'équipe de sécurité ne l'avaient pas détecté, car le serveur utilisait comme domaine la marque de l'événement marketing, jamais signalée et aujourd'hui oubliée, plutôt que le nom de l'entreprise.

Machine Translated by Google

Dans le répertoire de fichiers de ce serveur se trouvaient des clés Secure Shell (SSH) vieilles de plusieurs années, qui fournissaient encore un accès sécurisé au principal cluster de serveurs marketing de l'organisation. Une fois sur place, les pirates ont pu rapidement s'y attaquer et obtenir l'accès au domaine SharePoint et OneDrive. À ce stade, comme le révèlent les journaux récupérés ultérieurement, il y a eu une pause de 48 heures, probablement le temps pour les pirates de vendre leur accès à un groupe de rançongiciels.

La connexion SSH du serveur web abandonné était un événement « anormal ». La plateforme de gestion des incidents et des événements de l'équipe de sécurité l'a signalée comme telle avec le code « orange/anormal », le niveau d'alerte le plus bas. La plateforme a signalé des centaines d'autres événements orange ce jour-là et des dizaines d'autres classés « rouges/suspects ». Aucun n'a été classé « rouge clignotant/« hostile. » La demi-douzaine d'analystes de l'équipe de sécurité ont tenté de résoudre autant de problèmes que possible, mais personne n'a vérifié la connexion SSH anormale.

« Avec autant de faux positifs, il arrive que des erreurs passent inaperçues », a reconnu le RSSI. « En fin de compte, nous n'avons pas les effectifs nécessaires pour résoudre chaque signalement d'anomalie. »

L'autopsie, réalisée par une société de sécurité tierce, a révélé que les analyses et les attaques visant le serveur marketing abandonné provenaient de la même plage d'adresses IP que celle placée sur la liste noire du SOC, car elle était à l'origine des attaques par pulvérisation de mots de passe. Des liens, via la recherche dans la base de données Whois, menaient également vers la campagne d'e-mails de spear-phishing. L'inscription des adresses IP sur la liste noire n'a pas protégé le serveur abandonné, car…
en tant qu'actif informatique fantôme non enregistré et abandonné, il n'était pas soumis à la politique de sécurité de l'entreprise.

« Si seulement nous avions eu un moyen de trier ces alertes, de séparer le bon grain de l'ivraie, et la capacité de corréler les données des plus significatives, nous aurions peut-être pu « Ils ont repéré la connexion et ont stoppé la troisième attaque », a déclaré le RSSI lors de l'enquête interne post-mortem. De retour au cluster marketing principal avec accès au domaine après 48 heures, les pirates ont commencé à exfiltrer et à chiffrer les données.

Mettre les équipes de sécurité en première ligne

Cette vignette est fictive, mais le personnel de sécurité est régulièrement confronté à des attaques comme celles décrites ci-dessus. Aujourd'hui, même les équipes de cybersécurité des entreprises les mieux dotées en ressources sont confrontées à un rythme opérationnel de plus en plus intenable, avec peu de possibilités de procéder à un triage efficace et d'isoler les intrusions les plus dangereuses. L'accumulation de données sur l'état des systèmes et l'activité potentielle des attaquants n'est utile que dans la mesure où elles peuvent être analysées ; au-delà, elle ne fait qu'augmenter la taille de la botte de foin qui cache l'aiguille des menaces potentielles.

Combinez cette surcharge de données à la complexité croissante des systèmes informatiques d'entreprise modernes (infrastructures multicloud, outils multifournisseurs, conformité multijuridictionnelle) et vous obtenez un scénario d'échec, même pour les SOC les plus expérimentés et les mieux dotés en ressources. Ce scénario s'aggrave désormais avec l'intelligence artificielle générative (GenAI) utilisée par les attaquants pour déployer des attaques de spear-phishing personnalisées et soigneusement ciblées, d'une poignée à des centaines de cibles.

La bonne nouvelle, c'est que les entreprises peuvent changer la donne en matière de cybersécurité. En exploitant l'IA et l'apprentissage automatique (ML) dès le début du cycle de vie des alertes, elles peuvent atténuer les faux positifs incessants, optimiser leur flux de réponse aux incidents et aider les équipes de sécurité à accomplir leurs tâches critiques plus rapidement et plus efficacement.
L'intelligence artificielle peut améliorer la capacité des équipes de sécurité à mener une chasse proactive aux menaces en utilisant une surveillance à grande échelle de l'espace gris pour analyser l'activité pré-attaque et déterminer comment les attaquants prévoient de pénétrer un réseau.

Machine Translated by Google

Débordé sur deux fronts

L'ironie est que, dans notre exemple fictif, l'équipe de sécurité disposait de toutes les données nécessaires pour détecter et stopper l'intrusion. Elle ignorait simplement qu'elle les possédait et ignorait comment les exploiter. Ce constat est vrai dans une proportion étonnamment importante d'attaques réelles, et cela s'explique par le fait que les équipes de sécurité sont de plus en plus débordées sur deux fronts : la densité technologique et les ressources humaines.

DU CÔTÉ HUMAIN, L'ENJEU EST COGNITIF CONTRAINTES DE RESSOURCES :

Il est difficile de recruter du personnel de sécurité expérimenté et talentueux. Ce problème est particulièrement marqué dans des niches de spécialisation très demandées comme la sécurité cloud ou la sécurité de l'IA. Sur un marché du travail aussi concurrentiel, le roulement peut être problématique pour les praticiens débutants et intermédiaires, et les approches de développement des talents prennent des années et nécessitent des investissements importants.

Même les plateformes de gestion des informations et des événements de sécurité (SIEM) et de détection et réponse aux points d'extrémité (EDR) correctement calibrées génèrent un volume d'alertes ingérable. La grande majorité de ces alertes sont des faux positifs ou des preuves de menaces de sécurité courantes. L'intégration d'outils fournissant des données contextuelles est considérée comme une bonne pratique, mais elle peut générer des alertes en double si elle est mal réalisée. Même bien réalisée, l'intégration peut finir par remplacer la lassitude liée aux alertes par une lassitude contextuelle : un excès de données supplémentaires peut être accablant plutôt qu'instructif. Le tri et la résolution de ces alertes absorbent un nombre considérable d'heures d'analyste, même pour un SOC doté de ressources suffisantes et d'un personnel complet, et la charge cognitive liée au tri incessant des alertes peut entraîner des problèmes de rétention. Il existe également un coût d'opportunité : les heures d'analyste perdues à trier le bruit pourraient être consacrées à la recherche proactive des menaces les plus dangereuses.

Une équipe de sécurité qui laisse une file d'alertes définir son ordre du jour sera toujours sur la défensive. Le manque d'analyses signifie que les équipes de sécurité passent trop de temps à traquer des alertes qui peuvent ou non être la preuve d'une intrusion, sans savoir qui est à l'origine de ces alertes ni à quel point elles sont dangereuses.

SUR LE CÔTÉ TECHNIQUE, LES PROBLÈMES SONT ENCORE PLUS IMPORTANTS VARIÉ ET COMPLEXE :

Le partage de données sur la vitesse des machines reste encore une aspiration plutôt qu'une réalité. Pour des raisons complexes et diverses, de nombreuses organisations n'utilisent pas ou ne peuvent pas utiliser les formats STIX (Structured Threat Information eXpression) et TAXII (Trusted Automated eXchange of Intelligence Information) ou d'autres formats standard pour les données de cybermenaces, afin de les importer automatiquement dans les outils de défense. Sans ce type de partage de données en temps réel et à la vitesse des machines, les indicateurs de renseignement doivent être saisis manuellement dans les pare-feu ou les outils SIEM, souvent par copier-coller.

Les équipes de sécurité utilisent des outils et plateformes de plusieurs fournisseurs, souvent dotés chacun de leur propre tableau de bord et interface de contrôle. L'intégration de ces outils n'est pas aussi simple qu'elle devrait l'être, et certains outils de fournisseurs ne sont pas capables d'ingérer de manière transparente les données des produits concurrents, ou le font à un coût élevé.

Au-delà de l'équipe de sécurité elle-même, les environnements informatiques des entreprises mondiales modernes sont d'une complexité extraordinaire. Des appareils, plus ou moins fiables, doivent se connecter et se déconnecter du réseau à différents endroits. L'infrastructure, le stockage de données, les applications et les services sont répartis entre plusieurs fournisseurs de cloud (et parfois des centres de données sur site) et terminaux, gérés par des outils en constante évolution provenant de différents fournisseurs. L'intégration des outils des différents fournisseurs engendre souvent un niveau de complexité supplémentaire et peut entraîner une surcharge logicielle.

À cette complexité s'ajoutent les millions de points de données créés par les outils de cybersécurité modernes. L'ingestion et le traitement des données d'événements/journaux d'une grande entreprise peuvent représenter un défi informatique pour les SIEM et autres plateformes de sécurité.

Le modèle traditionnel en étoile pour l'équipe de sécurité, où les données sont ramenées au centre et analysées, puis les mesures défensives sont déployées de manière centralisée via des modifications des règles SIEM, de pare-feu ou EDR, n'est tout simplement pas adapté à une grande entreprise moderne compte tenu du volume de données impliquées.
Le coût et le calcul ne s'additionnent pas.

Le modèle défensif traditionnel, qui, lorsqu'il s'agit d'attaquants haut de gamme, se résume à supposer qu'ils ont déjà pénétré dans le réseau et à rechercher dans le réseau des traces qu'ils auraient pu laisser accidentellement lors de leurs déplacements, n'est pas non plus évolutif.
Cela laisse les équipes défensives en permanence sur la défensive.

Ces défis deviennent de plus en plus graves à mesure que les entreprises sont confrontées aux menaces croissantes des cyberattaques alimentées par l'IA. Des robots d'IA générative spécialement conçus pour la cybercriminalité, comme Evil GPT ou WormGPT, sont annoncés sur les forums de hackers du Dark Web depuis au moins deux ans, et une équipe de chercheurs de l'Université de l'Indiana a trouvé des exemples réels d'acteurs de la cybercriminalité utilisant des outils GenAI pour écrire des logiciels malveillants, générer des e-mails de phishing et créer des sites Web frauduleux.

L'intelligence artificielle peut améliorer la capacité des équipes de sécurité à mener une chasse proactive aux menaces en utilisant une surveillance à grande échelle de l'espace gris pour analyser l'activité pré-attaque et déterminer comment les attaquants prévoient de pénétrer un réseau.

Machine Translated by Google

Un problème de données, pas un problème de défense

La dure réalité est que les équipes de sécurité sont souvent trop débordées par leurs problèmes de données pour mettre en place une défense efficace. Le volume de données arrivant trop rapidement empêche les équipes humaines de distinguer rapidement les menaces pertinentes des informations superflues. De plus, les équipes de sécurité manquent d'informations sur la gravité des menaces que les acteurs cherchent à compromettre leur réseau. En exploitant les capacités croissantes de l'IA en matière d'analyse des données pour se concentrer sur les menaces pertinentes et tirer des conclusions sur les TTP des attaquants grâce à une surveillance à grande échelle de l'activité des groupes de menaces avant l'attaque, les équipes de cybersécurité peuvent enfin devancer leurs assaillants.

Faire taire le bruit

Lorsqu'ils sont déployés au début du cycle d'alerte, le ML et l'IA aident les équipes de détection des menaces à mieux gérer les milliers d'alertes dupliquées et pour la plupart faussement positives reçues quotidiennement de divers outils cybernétiques.

- Les outils ML utilisant l'apprentissage non supervisé peuvent regrouper les alertes en double provenant de différents outils et isoler les anomalies les plus susceptibles d'être importantes.

- La collecte d'étiquettes et la formation de modèles permettent aux outils d'IA utilisant l'apprentissage supervisé de prédire la probabilité d'un vrai positif, qui à son tour filtre dynamiquement des milliers d'alertes quotidiennes jusqu'à une poignée d'avertissements haute fidélité qui sont transmis à l'équipe de détection d'incidents pour examen.

Il est également possible d'utiliser un modèle d'apprentissage automatique pour prioriser les alertes critiques et les signaler comme essentielles, évitant ainsi aux analystes d'évaluer la probabilité d'une alerte. De puissants algorithmes d'IA permettent aux organisations d'automatiser ce processus en toute confiance, ce qui permet de déprioriser les événements improbables et de ne pas dépendre uniquement des humains pour évaluer la viabilité d'une alerte.

L'intégration de ces outils dans les flux de travail existants et leur personnalisation pour répondre aux besoins du système permettent aux analystes de se concentrer sur le traitement des véritables alertes positives, ce qui atténue les risques en diminuant le nombre d'alertes nécessitant une attention humaine et en diminuant la fatigue liée aux alertes.

Idées en action

Les entreprises privées et les agences fédérales utilisent déjà l'IA pour renforcer leurs cyberdéfenses.

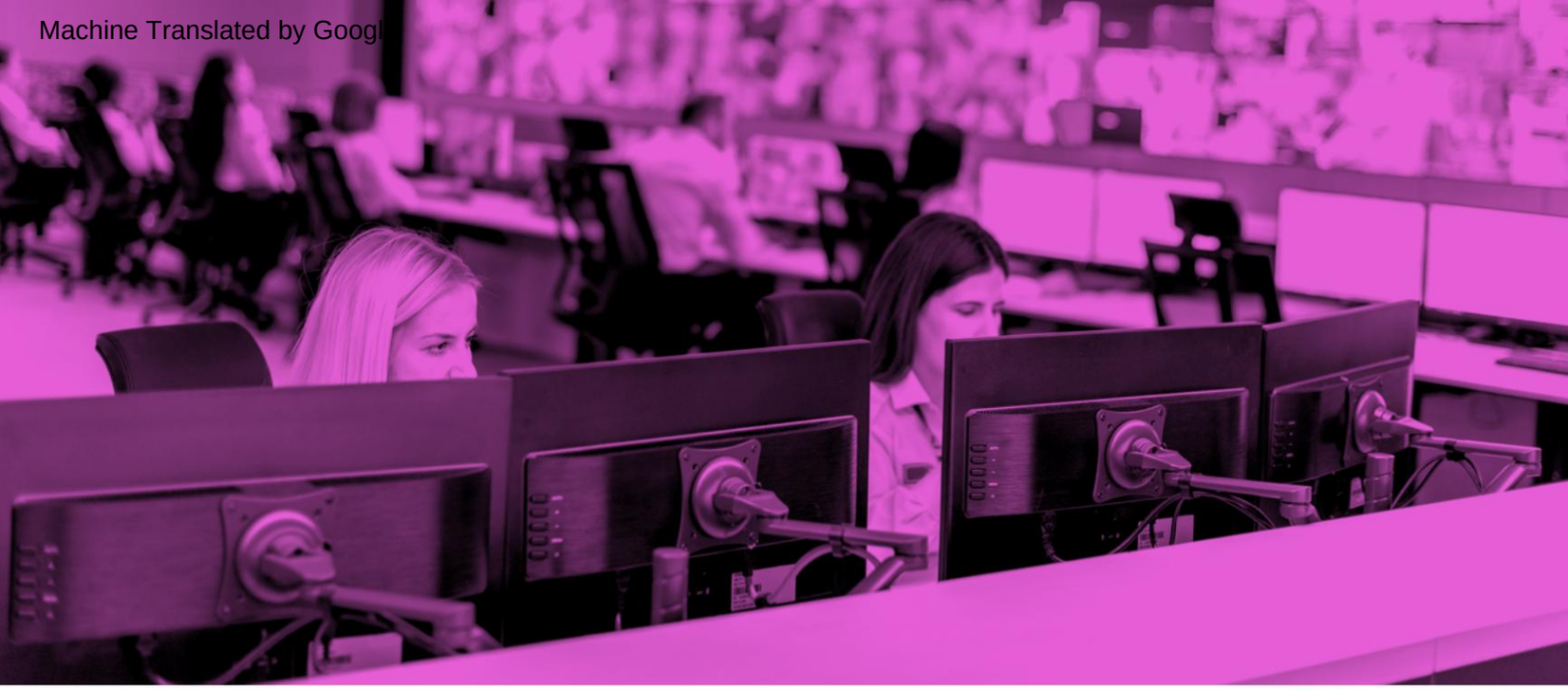
Un constructeur automobile mondial, par exemple, s'est donné pour mission d'identifier les failles de sa stratégie de sécurité, d'élaborer une feuille de route pour améliorer l'efficacité de ses opérations et d'accroître sa visibilité sur l'ensemble des menaces. L'échelle était un enjeu majeur : 1 200 sources de données uniques de cyber-informations ; de nombreux sites ; et des milliards de messages provenant d'outils cybernétiques chaque jour. Les analystes devaient déduire des schémas significatifs à partir d'ensembles de données complexes et consacraient des heures de travail considérables à l'analyse des faux positifs.

Le constructeur automobile a relevé ces défis en intégrant le ML et l'IA dès le début du cycle de vie des alertes. Il a également créé un modèle automatisé facile à déployer, rapidement et facilement, dans tout environnement réseau et pipeline de données cloud suffisamment volumineux pour gérer d'importants volumes de cyberinformations. Le projet a également mis en place une capacité de cyber-IA permettant aux utilisateurs de l'équipe de sécurité d'accéder à des produits personnalisés de big data, de ML et d'intelligence artificielle.

Ces solutions ont eu un impact immédiat et considérable. Au lieu de gérer un flux d'alertes complexe, l'équipe peut désormais se concentrer sur les véritables alertes positives et garantir la diffusion des événements de sécurité en quelques secondes, où que vous soyez sur la planète.

Au sein du gouvernement fédéral, une mission d'envergure et cruciale nécessitait un moyen plus efficace de détecter et de corriger les vulnérabilités. L'équipe a commencé à tester une solution utilisant l'IA pour intégrer des évaluations en temps réel des risques système à une solution de détection. Cette analyse des risques, alimentée par l'IA, permet de quantifier la manière dont un adversaire pourrait exploiter un système donné, améliorant ainsi la compréhension des risques par l'équipe de sécurité dans le cadre de la surveillance. L'application pilote a permis à l'équipe de détecter en quelques secondes les cyberattaques qui contournaient les défenses traditionnelles, tout en réduisant considérablement les faux positifs et la lassitude face aux alertes.

Machine Translated by Googl



Éliminer les goulots d'étranglement liés à la réponse aux incidents

L'IA et le ML peuvent contribuer à réduire les goulots d'étranglement et à lever les blocages dans la réponse aux incidents. Par exemple, certains incidents nécessitent le même type de résolution à chaque fois qu'ils se reproduisent. De plus, il n'est pas rare qu'un type familier de faux positif frappe un réseau dans des circonstances prévisibles.
Plutôt que d'envoyer ces incidents dans la file d'attente d'un analyste pour correction, les grands modèles de langage (LLM) peuvent les identifier et accélérer leur résolution.

Dans le cadre d'un processus d'enrichissement automatisé, un modèle LLM peut être intégré à une solution d'orchestration, d'automatisation et de réponse de sécurité pour initier une conversation par chat entre l'utilisateur et l'IA. L'IA reçoit le contexte de l'alerte et des instructions pour recueillir davantage d'informations auprès de l'utilisateur et fournir un résumé de la conversation, qui est ensuite ajouté au dossier. Un algorithme d'apprentissage automatique peut également être intégré à cette approche pour classer le type d'incident reçu comme alerte bénigne ou menace malveillante, en fonction des similitudes avec des incidents précédents.

Les LLM peuvent également être utiles aux équipes de sécurité. Associés à un outil comme Slack, ils permettent d'informer un analyste des dernières corrections de tickets ou de fournir un résumé des événements des 10 derniers jours. Du point de vue de l'expérience utilisateur, les LLM permettent de contacter les utilisateurs ayant fourni des informations dans un ticket, un processus qui prend actuellement beaucoup de temps aux analystes.

Plutôt que de consacrer des heures humaines à ce processus, l'IA peut interagir avec l'utilisateur pour identifier les lacunes et recueillir des informations supplémentaires dont l'analyste a besoin pour terminer l'enquête.

Tirer des enseignements de l'espace gris

Le plus grand cas d'utilisation potentiel de l'IA pour la cybersécurité pourrait être sa capacité à faire évoluer la chasse aux menaces d'un jeu de devinettes à grande échelle vers une approche axée sur le renseignement dans laquelle la sécurité les équipes exploitent de nouvelles sources de renseignements exploitables pour identifier et bloquer les TTP des attaquants avant qu'ils ne soient utilisés contre l'entreprise.

Avant de passer à l'action, les pirates préparent leur infrastructure (comme de faux sites de connexion pour les campagnes de phishing), développent ou peaufinent des logiciels malveillants et se livrent à d'autres activités qui laissent entrevoir de futures attaques. Généralement, ces activités ne sont pas menées dans l'infrastructure des attaquants (« espace rouge »), ni déployées à ce stade dans l'infrastructure des défenseurs (« espace bleu »). Elles interviennent plus tard, pendant l'attaque elle-même.

En revanche, ces activités de préparation d'attaques se déroulent généralement dans des infrastructures compromises ou louées, temporairement contrôlées par les pirates, mais n'appartenant pas à ces derniers (espaces gris). Ces emplacements peuvent être surveillés via l'Internet public, et de nombreux analystes de menaces expérimentés ou compétents suivent probablement quelques-uns de ces emplacements utilisés à cette fin par les acteurs malveillants, analysant les données de leurs activités pour établir des prévisions éclairées sur les futures campagnes d'attaques.

Grâce aux capacités croissantes de l'IA, les activités de surveillance et d'analyse peuvent désormais être déployées à grande échelle. Des analyses à l'échelle d'Internet et d'autres techniques complètes de collecte de données (par exemple, l'analyse de tous les domaines Internet créés au cours des dernières 24 heures) peuvent être utilisées pour détecter des preuves d'activités malveillantes, qui peuvent ensuite être surveillées. L'IA peut tirer des conclusions de ces données de surveillance pour définir les TTP les plus susceptibles d'être utilisés lors d'attaques futures.

Les données peuvent ensuite être croisées avec les informations sur le réseau de l'entreprise (ses vulnérabilités et la posture du système) afin de créer des méthodes de détection et de prévention à la volée. Ces méthodes reposent sur l'utilisation de l'IA/ML pour comparer la posture actuelle du système aux vulnérabilités que les attaquants prévoient d'exploiter et pour concevoir des contre-mesures implémentables par les outils de sécurité.

Le plus grand cas d'utilisation potentiel de l'IA pour la cybersécurité pourrait être sa capacité à faire évoluer la chasse aux menaces d'un jeu de devinettes à grande échelle vers une approche basée sur le renseignement.

Donner aux équipes de sécurité les moyens de réussir

Pour revenir à notre scénario fictif, comme indiqué précédemment, l'équipe avait accès à toutes les données nécessaires pour empêcher la troisième attaque, mais elle ignorait qu'elle les possédait et ne disposait pas des outils nécessaires pour les exploiter afin de se défendre. En appliquant les approches décrites ici, notre équipe de sécurité fictive aurait été vouée au succès, et non à l'échec.

- Le tri des alertes par IA/ML, l'élimination des faux positifs et la résolution automatique auraient réduit les centaines de rapports orange/anormaux à un nombre où les analystes auraient pu enquêter sur chacun d'eux, trouver le serveur marketing abandonné et bloquer la troisième attaque.
- Corrélation des données des deux premières attaques, soit par des analystes libérés du « travail répétitif par IA/ML » (soit par IA/(ML lui-même) aurait fourni des alertes de renseignement qui auraient pu empêcher la troisième attaque.
- La surveillance des opérations de l'espace gris des acteurs de la menace aurait fourni des données qui auraient pu bloquer automatiquement les attaques par pulvérisation de mots de passe et auraient pu identifier les TTP utilisés par les intrus dans l'attaque à partir du serveur marketing.

L'IA fait l'objet de beaucoup de battage médiatique, mais il s'agit de cas d'utilisation où une application judicieuse des outils d'IA peut transformer le paysage de la sécurité pour les grandes entreprises.

Tony Sharp dirige la pratique des solutions de cybertechnologie commerciale de Booz Allen.

Joe Gillespie est un dirigeant senior de l'activité Cyber nationale de Booz Allen.

Matt Costello dirige les activités d'analyse commerciale et d'IA de Booz Allen ainsi que nos pratiques en matière de menaces internes.

Mike Saxton est le directeur de l'activité de défense informée par l'adversaire de Booz Allen et dirige l'équipe fédérale de recherche de menaces, d'investigation numérique et de réponse aux incidents.

Rita Ismaylov dirige l'activité d'IA commerciale de Booz Allen en mettant l'accent sur la conception de solutions d'IA et en aidant les clients à développer leurs capacités d'IA.

LECTURE RAPIDE

Les équipes de sécurité sont confrontées à des défis techniques et humains croissants : une pénurie de personnel qualifié, un volume écrasant d'alertes dans des environnements multi-cloud complexes et la montée des cyberattaques alimentées par l'IA mettent les défenseurs de plus en plus sur la défensive.

L'IA et l'apprentissage automatique peuvent transformer la cybersécurité en filtrant les faux positifs au début du cycle de vie des alertes et en automatisant les réponses aux incidents de routine, permettant ainsi aux analystes humains de se concentrer sur les menaces graves.

En utilisant l'IA pour surveiller les activités de l'espace gris (où les pirates préparent leurs attaques), les équipes de sécurité peuvent passer d'une défense réactive à une chasse proactive aux menaces, en identifiant et en bloquant les attaques potentielles avant qu'elles ne se produisent.

Machine Translated by Google

MISSION À L'HONNEUR : L'ESPACE

Prendre le terrain Systèmes hors sol

POUR LE SEGMENT SOL SPATIAL, LA SCIENCE DES DONNÉES C'EST DE LA SCIENCE DE FUSÉE

Josh Perrius et Ginny Cevasco

Machine Translated by Google

Guerre spatiale commerciale en raison de l'utilisation d'images d'entreprises privées pour le suivi et le ciblage. Ce conflit a

La guerre entre la Russie et l'Ukraine est sans doute la première démontré l'intérêt de connaître la situation au sol et a mis en lumière le rôle du domaine spatial pour la région indo-pacifique critique et les points chauds du monde.

Aujourd'hui, les pays du monde entier accélèrent leurs programmes spatiaux, ce qui renforce l'urgence alors que les États-Unis accélèrent la modernisation de l'espace.

La prolifération des satellites de nouvelle génération alimente la demande d'infrastructures de nouvelle génération. Les systèmes terrestres virtuels, qui utilisent une infrastructure logicielle et le cloud computing pour contrôler les satellites, représentent un progrès considérable pour les opérations spatiales. Ces systèmes virtuels ne sont pas liés à une seule installation physique. Ils sont plus sûrs et plus faciles à mettre à jour que les systèmes traditionnels dépendants du matériel. Ils permettent également une intégration transparente de l'intelligence artificielle (IA) et de l'apprentissage automatique aux opérations spatiales. Ces avancées permettent aux opérateurs de traiter les données collectées par les satellites plutôt que de simplement les stocker ou de les supprimer car elles sont inutilisables. Il en résulte une mine d'informations précieuses qui peuvent améliorer la prise de décision des opérateurs en temps réel.

Les systèmes terrestres réfléchissent

Si les constellations agiles de petits satellites captivent l'imagination par leur résilience et leur flexibilité, c'est le « cerveau » – le système terrestre – de chaque réseau qui dirige la mission et en assure le succès. Le commandement et le contrôle (prise de décision), la gestion de la mission (planification, tests et opérations), ainsi que le traitement et la diffusion des données dépendent tous du système terrestre et de ses opérateurs.

L'automatisation des activités clés permettra aux opérateurs de se concentrer sur les décisions critiques et d'intégrer harmonieusement des systèmes actuellement cloisonnés. La modernisation de ces fonctions est essentielle pour maintenir les ambitions spatiales américaines à un niveau élevé.

Bien que 150,4 milliards de dollars aient été dépensés en technologies du segment terrestre en 2023 selon un communiqué de presse de juin 2024 Selon la Satellite Industry Association, de nombreuses organisations spatiales doivent encore faire face à des équipements hérités.

De plus, rien ne garantit que les nouveaux systèmes terrestres utilisent les dernières innovations logicielles nécessaires pour rendre les systèmes intelligents, évolutifs et sécurisés.
C'est parce que les nouveaux systèmes terrestres sont souvent inclus dans le contrat d'un système spatial global, ce qui signifie que les entrepreneurs habitués à construire des systèmes existants peuvent construire le système en utilisant des techniques qu'ils connaissent déjà plutôt que les dernières innovations logicielles.

Pourquoi les opérateurs ont besoin de systèmes agiles

Imaginez que vous êtes opérateur satellite au sein d'une organisation militaire ou de renseignement. Vous travaillez probablement dans une station terrestre physique et effectuez des tâches telles que la surveillance par satellite d'une région donnée, le suivi de satellites et d'autres ressources spatiales, ou la fourniture d'images satellite pour soutenir une opération militaire.

Pour ce faire, vous dirigez un satellite à l'aide d'instructions, ou « tâches », qui comprennent plusieurs actions : définir la zone d'intérêt, trouver une constellation disponible, choisir entre images radar et optiques, déterminer l'angle de vue, etc. Vous suivez différents actifs sur plusieurs écrans, ce qui complexifie votre travail.

Imaginons qu'un satellite repère les troupes ennemies se déplaçant au sol près d'une zone contestée. Ce satellite n'étant pas prévu pour effectuer un nouveau survol de la zone avant huit heures, vous décidez de confier la reconnaissance à un autre satellite. C'est un processus inefficace et chronophage.

Vous devez d'abord décider si vous souhaitez faire appel à un fournisseur commercial ou à une source confidentielle. Ensuite, selon les ressources disponibles et les conditions indépendantes de votre volonté, la mise en place d'un ou plusieurs satellites et le téléchargement des images peuvent prendre de quelques minutes à quelques heures.

Par exemple, si le temps est partiellement couvert dans cette région, il vous faudra un radar à synthèse d'ouverture pour percer la couverture nuageuse. Il vous faudra également un satellite à haute résolution.

Le pouvoir de l'ouverture Cadres de données

Le développement d'une architecture ouverte offre des avantages immédiats pour les systèmes au sol :

- Contrairement à un système monolithique, un système construit sur des cadres ouverts peut être mis en œuvre étape par étape, offrant ainsi des avantages rapidement.
- Une fois que les agences spatiales ont migré vers un système modernisé, un processus DevSecOps discipliné garantit une intégration continue et un déploiement continu avec des déploiements inter-domaines automatisés.
- La cybersécurité intégrée atténue les menaces.
- Un cadre de données ouvert permet aux équipes d'intégrer les avancées de partout, qu'il s'agisse d'un sous-traitant de la défense ou d'une startup de la Silicon Valley.

Machine Translated by Google

caméra — et des solutions logicielles qui lui permettent d'identifier les zones couvertes et d'éviter d'y collecter des données inutiles — pour identifier les équipements en transit.

Vous ressentez la pression, car la situation au sol évolue à chaque instant. Pendant ce temps, vous savez que la cyberforce adverse pourrait tenter de pénétrer l'infrastructure vieillissante de la station terrestre ou de détruire complètement le système.

Rationalisation des opérations grâce à la centralité des données

La bonne nouvelle pour les opérateurs est que l'ingénierie des données permet des avancées logicielles offrant de nouvelles capacités et une plus grande flexibilité. Selon la stratégie de données du Département de la Défense (DOD), Publié en septembre 2020, le succès commence par la centralité des données, en plaçant les données au centre de l'organisation et de ses systèmes, permettant aux États-Unis d'agir sur les données plus rapidement que leurs adversaires.

Cette approche peut être résumée comme signifiant que le réseau doit prendre en charge les données plutôt que l'inverse.

Pour les systèmes terrestres, cette transition peut être réalisée en construisant des systèmes à architecture ouverte capables de s'adapter à l'évolution des missions. Directive de politique spatiale du Département de la Défense de septembre 2023. souligne la nécessité d'accélérer la transition vers des architectures plus résilientes et les mandats du DOD approches modulaires à systèmes ouverts.

Les systèmes à architecture ouverte offrent une sécurité Zero Trust intégrée, offrant des contrôles d'accès précis et permettant une évolution continue. Mis en œuvre par des experts techniques connaissant les subtilités de la mission, ils permettent aux agences spatiales de construire un système autour d'objectifs fondamentaux tout en conservant des capacités flexibles pour s'adapter aux priorités et défis futurs.

Les avantages du virtuel Systèmes au sol

Ajoutez une plateforme à architecture ouverte au cloud et vous avez la possibilité de contourner entièrement les infrastructures physiques. Les opérateurs avant-gardistes optent déjà pour la virtualisation, une approche cloud utilisant un environnement informatique virtuel. Cette option offre une flexibilité d'hébergement en tout lieu et une sécurité renforcée, développée plus rapidement que les structures physiques et à moindre coût.

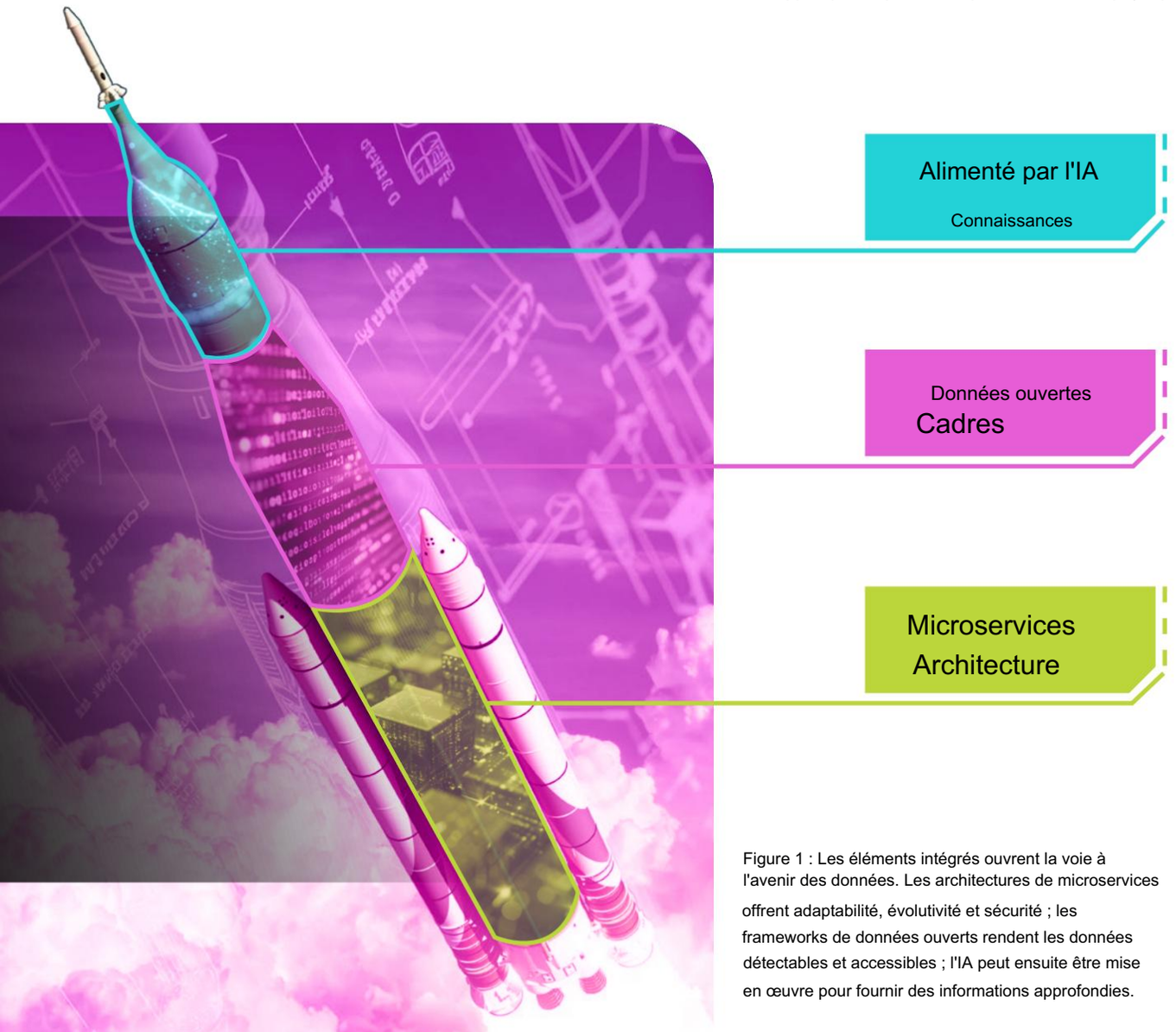


Figure 1 : Les éléments intégrés ouvrent la voie à l'avenir des données. Les architectures de microservices offrent adaptabilité, évolutivité et sécurité ; les frameworks de données ouverts rendent les données détectables et accessibles ; l'IA peut ensuite être mise en œuvre pour fournir des informations approfondies.

Machine Translated by Google

Avec un système terrestre virtualisé, les parties prenantes bénéficient d'avantages dans toutes les fonctions, réalisant :

- Commande et contrôle intelligents et automatisés pour des déplacements de satellites plus rapides, une plus grande précision et des analyses qui incluent des plans d'action
- Gestion de mission améliorée pour une planification plus rapide et des mises à niveau et une intégration plus fluides des flux de données des capteurs entre les systèmes et les constellations
- Transformation rapide des données pour une collecte, un traitement, un stockage et une diffusion rapides des données
- L'IA et l'apprentissage automatique pour faire progresser en permanence les capacités avec des modèles qui évoluent au rythme de la mission

Un système terrestre spatial virtuel utilisant une plate-forme multicloud offre aux organisations la flexibilité nécessaire pour adopter de nouvelles technologies et s'adapter à l'évolution des exigences de mission. Il permet aux gestionnaires, opérateurs et techniciens de satellites de gérer les missions depuis un seul ordinateur portable grâce à une architecture plug-and-play qui offre à la fois une sécurité Zero Trust et une résilience pour rester opérationnel après une attaque. Autre point crucial, l'automatisation intelligente réduit le processus de gestion des missions spatiales de plusieurs jours à quelques heures, voire quelques minutes.

Les éléments des architectures ouvertes

Tout comme les fusées sont propulsées par un carburant liquide composé d'éléments tels que l'hydrogène et l'oxygène, les systèmes terrestres modernisés, qu'ils soient traditionnels ou virtuels, sont propulsés par des éléments centrés sur les données.

Les agences fédérales peuvent intégrer ces éléments même dans les systèmes existants, leur offrant ainsi les avantages de la modernisation que la Space Force, en tant qu'agence la plus récente, utilise déjà comme base sur laquelle s'appuyer.

Architecture de microservices : la décomposition de services monolithiques en éléments modulaires et indépendants permet l'évolutivité et la personnalisation. Par exemple, les parties prenantes peuvent adapter un service conteneurisé existant tel quel, le remplacer ou l'adapter à un usage spécifique. Les interfaces de programmation d'applications (API) ouvertes garantissent l'interopérabilité avec toutes les technologies et permettent des mises à jour rapides pour tirer parti des avancées technologiques.

Plateforme de données ouvertes : cet écosystème de données modulaire ingère, traduit, stocke, organise et rend les données détectables et accessibles. Il comprend des outils DevSecOps avec un framework de déploiement ; un pipeline d'intégration et de déploiement continus (CI/CD) ; une plateforme de données qui intègre et stocke les nouveaux flux de manière sécurisée ; et un catalogue de données centralisé, facilitant la découverte grâce à des normes de métadonnées communes.

Services partagés inter-domaines — Face à l'intensification des menaces mondiales, les opérations inter-domaines et conjointes deviennent de plus en plus cruciales. Le partage des données pertinentes pour la mission, qu'elles soient de niveau hiérarchique supérieur ou inférieur, doit donc être accéléré et simplifié. Parallèlement, les parties prenantes doivent fusionner les données multi-renseignements et multi-domaines pour obtenir des informations plus nuancées.

Architectures Zero Trust : L'application d'une sécurité granulaire aux données spatiales est essentielle pour protéger les ressources spatiales et garantir que les partenaires puissent partager des données en toute sécurité, à différents niveaux de sécurité. Pour assurer une cybersécurité efficace et un développement rapide des systèmes terrestres, les ingénieurs données doivent s'appuyer sur une plateforme garantissant les principes fondamentaux du Zero Trust. supposer une violation, ne jamais faire confiance, toujours vérifier et autoriser uniquement l'accès le moins privilégié sont intégrés dès le départ.

Transformer les missions spatiales

Les cadres de données ouverts sont essentiels, car ils permettent aux organisations d'intégrer les données cloisonnées qu'elles collectent en tirant parti des opérations d'apprentissage automatique (MLOps).
la capacité de créer, de former et d'ajuster des modèles d'IA pour obtenir des informations sur ce qui s'est passé et sur la manière de réagir.

Revenons au scénario où vous êtes l'opérateur.
Pensez à la différence que cela ferait d'être informé d'une situation et de recevoir des recommandations sur les mesures à prendre.

- Pour les opérations de défense, un modèle peut intégrer des images multi-renseignements d'une région pour analyser les tendances et prédire la probabilité d'une attaque militaire.
- Pour le changement climatique, un modèle peut intégrer des événements passés et des informations provenant de divers capteurs pour fournir une évaluation plus complète de l'impact environnemental dans une certaine zone.

Intégration de grands modèles linguistiques. Le cadre centré sur les données offre des processus sécurisés et reproductibles, avec un pipeline DevSecOps directement connecté aux données. Cette approche permet aux organisations spatiales de déployer rapidement des solutions d'IA et d'exploiter les avantages des grands modèles linguistiques (LLM), des algorithmes d'apprentissage profond capables de résoudre des problèmes complexes.

De plus, les stations terrestres spatiales virtuelles tournées vers l'avenir peuvent fournir la puissance des LLM en réseau.
Ces algorithmes, chacun formé sur de vastes ensembles de données, partagent des connaissances pour générer des informations rapides et fournir des plans d'action recommandés.

Accélérer la mission pour vous, l'humain

Reprenons l'exemple où vous êtes opérateur d'un satellite observant les mouvements de troupes en contrebas. Au lieu d'être dans une installation vieille de plusieurs décennies, jonglant entre plusieurs écrans, vous êtes désormais à distance, travaillant sur votre ordinateur portable.

Grâce à la virtualisation et à l'automatisation, vous vivez une situation très différente. Le système terrestre virtuel vous a alerté d'un mouvement inhabituel de troupes dans la zone et vous a fourni une liste de satellites commerciaux disponibles pour l'observation de la Terre, ainsi que des informations clés telles que le coût d'utilisation de chacun, la fidélité d'image attendue et le temps de séjour à prendre en compte. Enfin, il vous recommande une marche à suivre en deux étapes :

Machine Translated by Google

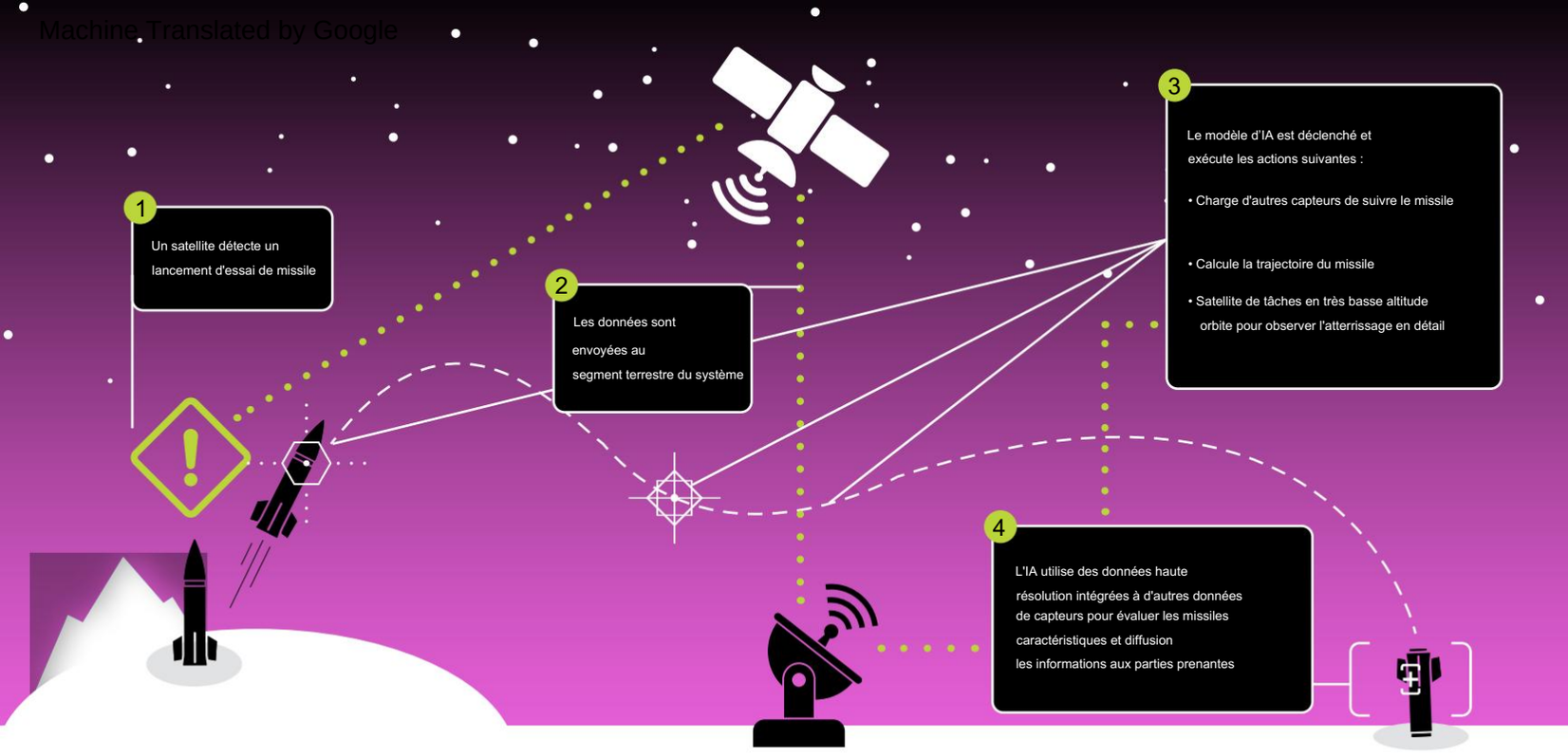


Figure 2 : L'application de l'IA à chaque phase des opérations spatiales traduit les données brutes en informations exploitables et réduit le temps entre l'analyse et l'action.

- Demandez à un satellite commercial d'observation de la Terre et à un satellite radar classifié d'effectuer un survol.
- Informer les alliés dans la zone du mouvement des troupes et de ses coordonnées.

Vous examinez la recommandation et appuyez sur Exécuter. Le système virtuel exécute automatiquement les deux parties de la recommandation. En quelques minutes, les navires de guerre à proximité se dirigent vers la zone dans une démonstration de force, et les troupes adverses, prises au dépourvu par cette action rapide, commencent à se disperser.

Ce n'est qu'un exemple de la manière dont des systèmes terrestres virtuels intelligents, évolutifs et sécurisés peuvent aider les humains à réaliser la seule chose qui soit meilleure que de gagner une guerre : éviter complètement le conflit grâce à une dissuasion efficace.

Josh Perrius et Ginny Cevasco sont des dirigeants seniors de l'activité National Security Space de Booz Allen.

LECTURE RAPIDE

La prolifération des petits satellites alimente la demande de systèmes terrestres basés sur le cloud qui permettent aux agences spatiales d'adopter des capacités avancées et d'éviter les risques de cybersécurité des installations physiques.

Un système spatial virtuel au sol utilisant une plateforme multicloud et des architectures plug-and-play permet de gérer les missions spatiales sur un seul ordinateur portable et peut réduire le processus d'attribution des tâches aux satellites de plusieurs jours à quelques heures, voire à quelques minutes.

Grâce aux systèmes terrestres virtuels, les cadres de données ouverts permettent aux organisations de tirer parti des opérations d'apprentissage automatique (MLOps) : la capacité de créer, de former et d'ajuster des modèles d'IA pour obtenir des informations sur ce qui s'est passé et sur la manière de réagir.

Machine Translated by Google

Sensema RÉIMAGINÉ

Découvrez comment les systèmes de nouvelle génération peuvent surpasser les menaces urgentes

Don Polaski, Marissa Beall et Christopher Castelli

Machine Translated by Google

roi

Analyste du renseignement

À l'aube, Grace, une toute

agence de renseignement de premier plan, elle se connecte à son poste de travail au siège. Depuis son bureau à Washington, elle porte son regard ultra-secret sur la région indo-pacifique, à l'autre bout du monde. C'est la même routine qu'elle a suivie pendant trois ans à ce poste. Mais ce matin, 3 février 2027, c'est différent. Elle reçoit un e-mail urgent de son superviseur. La suite, elle ne peut s'arrêter. Soudain, ses sourcils se froncent, ses yeux s'écarquillent, sa mâchoire se décroche et elle halète.

Le titre est clair : « La Chine achète une île inhabitée des Fidji pour y construire une base militaire. » L'information provient du bureau pékinois d'un grand quotidien américain. « Une société de développement chinoise liée au gouvernement chinois et à l'Armée populaire de libération a annoncé aujourd'hui avoir récemment acheté l'île inhabitée de Cobia au gouvernement fidjien pour 850 millions de dollars », peut-on lire dans l'article. « Les analystes de sécurité occidentaux estiment que la Chine envisage d'utiliser l'île pour construire une base militaire permanente dans le Pacifique Sud, à 5 000 km au sud-ouest d'Hawaï. »

Cette nouvelle signifie que la République populaire de Chine (RPC) peut renforcer sa projection de puissance dans les îles du Pacifique, une région d'importance stratégique, en élargissant la présence de son armée. l'Armée populaire de libération (APL) — près du sol américain et australien.

C'est le genre de surprise que Grace et ses collègues de la communauté du renseignement (CI) cherchent toujours à éviter. Ils savent au fond d'eux-mêmes qu'ils doivent se concentrer sur des cibles difficiles pour recueillir des informations sur les plans adverses qui, autrement, passeraient inaperçues, comme le recommande un rapport du Centre d'études stratégiques et internationales (CSIS). Une cible difficile est « une personne, une nation, un groupe ou un système technique » qui représente une menace potentielle et un défi de taille pour la collecte de renseignements : il est « souvent hostile aux États-Unis ou fortement protégé, et doté d'une capacité de contre-espionnage bien rodée ». Dans ce cas précis, la RPC a réussi à maintenir les Éta

« C'est pour ça qu'on appelle ça le défi du rythme », se dit Grace sans conviction. Ce n'est pas une consolation.

Machine Translated by Google

La vérité dans la fiction

Ce scénario imaginaire commence par un titre fictif emprunté à un rapport sur les tendances mondiales du National Intelligence Council de 2017 . Derrière notre système inventé se cache le besoin réel du circuit intégré d'anticiper les surprises en accélérant sa capacité à collecter, analyser et interpréter de vastes quantités de données. Ce défi s'intensifie à mesure que le nombre et la qualité des capteurs augmentent partout dans le monde.

Bien que le regard de Grace soit rivé sur l'Indo-Pacifique, aucune puissance étrangère n'a le monopole de l'insondabilité. Il y a plusieurs décennies, Winston Churchill décrivait la difficulté de prévoir les actions russes comme « une énigme enveloppée de mystère au cœur d'une énigme » – et cela semble toujours juste. Pour relever l'ensemble des défis de sécurité nationale à travers le monde, les analystes et les combattants en communication interétatique doivent donner un sens à des situations complexes et incertaines – et pour ce faire, ils ont besoin de systèmes d'analyse de données capables de collecter et d'analyser des données à une échelle exponentielle.

Grace remplace les analystes toutes sources, véritables spécialistes de la surveillance de l'influence étrangère de la RPC. Ces analystes examinent et analysent toutes sortes de données pour évaluer, interpréter, prévoir et expliquer divers enjeux et développements de sécurité nationale, qu'ils soient régionaux ou fonctionnels. Ils utilisent l'ensemble des outils, techniques et procédures toutes sources pour fusionner tous les renseignements disponibles en un produit complet, conçu pour répondre aux éléments d'information essentiels (EEI) au niveau de l'unité et aux besoins prioritaires en renseignement (PIR) au niveau du commandement.

La construction de sens est la capacité cognitive fondamentale que les analystes humains utilisent pour comprendre les évolutions émergentes et anticiper les événements futurs. Ce n'est pas le travail d'un analyste isolé, mais le fruit de la fusion de nombreux points de vue. La technologie joue un rôle de plus en plus important. Dix ans après les attentats du 11 septembre, l'Intelligence Advanced Research Projects Activity (IARPA) a décrit la construction de sens. comme « la remarquable capacité humaine à détecter des tendances dans les données et à en déduire les causes sous-jacentes, même lorsque les données sont rares, bruyantes et incertaines ». L'IARPA a également appelé au développement de nouveaux outils d'analyse automatisés conçus pour reproduire les atouts de cette capacité. Une stratégie de l'IC de 2019 pour l'augmentation de l'intelligence par les machines a défini la création de sens comme « un processus de compréhension dans des situations de grande complexité », préconisant la construction de modèles partagés « pour jeter les bases de la confiance entre les équipes humaines et les équipes machines ».

Si l'équipe de notre scénario hypothétique avait pu passer au peigne fin de vastes quantités de données de manière plus efficace et efficiente, elle aurait peut-être découvert plus tôt l'accord en préparation entre la RPC et les Fidji, permettant ainsi aux États-Unis de gérer de manière proactive les risques associés et peut-être même d'en façonner le résultat.

Dans cette première version de l'histoire, les capacités de compréhension dont dispose l'équipe ne sont pas aussi robustes qu'elles devraient l'être. Le CI est encore en train de passer d'approches axées sur la lutte antiterroriste à de nouvelles capacités techniques conçues pour la collecte et l'analyse de données contre des cibles difficiles et pour relever le défi du rythme. Réimaginons maintenant notre scénario, mais cette fois avec des systèmes de compréhension transformés déjà en place.

La création de sens réinventée . Six mois plus tard, Grace est assise en face de son superviseur dans une salle de réunion quelconque du siège social.

Une première analyse des signaux collectés, réalisée par un modèle de langage étendu (MLE) affiné, une forme d'intelligence artificielle (IA), a déclenché une alerte majeure concernant des cibles difficiles. Il est désormais temps que des analystes humains mènent l'enquête.

« L'APL et cette société de développement discutent. Je ne sais pas pourquoi », dit le superviseur en tendant un dossier à Grace. « Nous devons identifier toute opération potentielle. C'est là que vous intervenez. »

Grace regarde les photos. La société de développement est dirigée par un célèbre officier de renseignement chinois « à la retraite », une cible très délicate : rarement aperçue, jamais entendue. Les autres cibles sont des dirigeants de l'APL travaillant dans des installations hautement sécurisées.

« Vous aurez également accès à ces ressources », ajoute le superviseur, énumérant des outils aux noms sensibles et non répétables. La conversation ne s'attarde pas sur la manière dont ces outils incluent de nouveaux algorithmes pour renforcer la collecte, des capteurs plus puissants avec une plus grande puissance d'analyse en périphérie, des modèles de vision par ordinateur pour capturer de nouveaux objets ou détecter des changements dans des zones clés, des agents LLM pour simplifier le traitement d'énormes quantités de données, et des services d'analyse combinant signaux commerciaux et imagerie satellite.
À l'heure actuelle, l'important est que les outils aident Grace et son équipe à collecter rapidement les données pertinentes et à les relier. Ils synthétiseront rapidement les données, présenteront des options aux analystes et fonctionneront comme des assistants.

Pour recueillir des renseignements, Grace cible des individus clés, leurs organisations et les systèmes techniques concernés (par exemple, les appareils et équipements utilisés par les cibles). Les semaines passent. Ils se retrouvent à la hâte lorsque Grace annonce une avancée décisive. Plusieurs cibles discutent des Fidji, l'une d'elles mentionnant même un lieu précis : l'île de Cobia.
En forme de croissant de lune et bordée de grands arbres, l'île est un cratère volcanique submergé. Les touristes intrépides s'y rendent pour la randonnée, la plongée avec tuba et le kayak.

« L'APL préférerait peut-être y stationner des navires de guerre », dit le superviseur. « Nous aurons besoin de nouvelles images satellites aériennes. » L'équipe élabore d'autres plans de collecte et commence à les mettre en œuvre. Il s'avère que l'assistant IA a déjà anticipé le besoin et a commandé et reçu des images satellites commerciales de l'île. Mais un bref contretemps survient : un bug.

Sur les images aériennes, les eaux environnantes sont claires, mais une partie de l'île apparaît floue, presque camouflée. Ce n'est peut-être pas un bug. La vision par ordinateur analyse les pixels et Grace statue. La cible devient juste assez nette pour confirmer que quelqu'un cache habilement quelque chose. Mais quoi ?

Grace se tourne vers un collègue, Connor, responsable de la collecte de données. Il aide les analystes toutes sources à obtenir les données de renseignement nécessaires pour répondre à des questions clés. Constatant la nécessité de collecter davantage d'images et de signatures électroniques dans la zone, Connor utilise un drone pour obtenir une meilleure vue sous plusieurs angles.

Machine Translated by Google

Les nouvelles images 3D arrivent. Grace ouvre le fichier. Soudain, ses sourcils se froncent, ses yeux s'écarquillent, sa mâchoire tombe et elle halète.

« Ah ! » Une nouvelle structure se cache dans la magnifique forêt de la plage. Le bâtiment présente une conception atypique. Son empreinte est relativement petite, mais peut-être le début d'un projet plus vaste.
De plus, des signes d'un récent déversement de pétrole ou de produits chimiques sont présents sur le site. On ignore si les habitants ont déjà remarqué la fuite. Même si c'est le cas, ils ignorent peut-être que la contamination se propage derrière la structure jusqu'aux sables blancs et aux eaux cristallines.

En approfondissant, l'équipe utilise l'apprentissage automatique (ML) Des algorithmes analysent les signaux provenant de la zone afin de déterminer s'ils peuvent être liés à des acteurs connus. Les résultats indiquent que des membres de la société de développement clandestine se trouvent probablement sur le site. On les entend dire que la RPC envisage d'acheter l'île. Le superviseur de Grace est ravi.

« Si j'étais citoyen des Fidji, je voudrais être informé de la pollution qui menace l'environnement vierge », explique le superviseur.
« Excellent travail. » Les dirigeants du secteur touristique et de la communauté environnementale fidjiens apprennent rapidement qu'une marée noire s'est produite sur l'île. Avant que la société de développement soutenue par la RPC ne puisse conclure un accord pour l'acquisition de l'île, la population fidjienne exprime de vives inquiétudes, ce qui modifie la stratégie du gouvernement fidjien, qui hésite désormais à vendre. De plus, le travail de l'équipe a établi un modèle de vie pour les cibles de collecte. À l'avenir, le CI pourra s'appuyer sur ce modèle pour identifier et anticiper des risques similaires ailleurs dans la région.

Transformer les capacités de création de sens

Il ne s'agit là que d'un scénario hypothétique impliquant des cibles concrètes. D'autres pourraient être très différents. Il est urgent d'identifier, d'analyser et de suivre les évolutions émergentes à travers le monde. La stratégie de commandement et de contrôle interarmées (JADC2) de l'armée américaine privilégie la compréhension afin de transformer les données en informations et les informations en connaissances grâce à « la capacité de fusionner, d'analyser et de restituer des données et des informations validées provenant de tous les domaines et du spectre électromagnétique ».
Dans le cas malheureux d'une crise ou d'un conflit militaire, les capacités de compréhension pourraient rapidement évoluer de certaines manières. Mais il n'y a pas de temps à perdre. De plus en plus, les menaces émanant des États-nations prennent la forme d'actions coercitives ou subversives, bien en deçà du seuil d'un conflit armé.
Il est désormais crucial de développer et de renforcer les capacités de compréhension pour la sécurité nationale et la stabilité mondiale.

Globalement, le CI doit adopter, acquérir ou développer la technologie adéquate pour transformer ses capacités d'analyse et de détection, afin de pouvoir collecter et analyser des données contre des cibles difficiles malgré des capacités avancées de surveillance et de contre-espionnage adverses. La nature des conflits entre pairs rend cette modernisation continue d'autant plus difficile. Ces systèmes et ces analyses avancées doivent fonctionner dans des environnements à faible bande passante (DDIL) perturbés, déconnectés et intermittents. Ces contraintes nécessitent de nouvelles approches de développement et d'exploitation.
Par exemple, un rapport du CSIS recommande de recourir à des équipes de collecte avancées pour rapprocher la collecte et l'analyse basées sur l'IA des opérateurs dans les zones contestées. Il est essentiel de déployer ces capacités à la périphérie pour maintenir les analyses avancées requises, même lorsque les adversaires s'efforcent de neutraliser les systèmes de mission américains.

> “ Le besoin d’une nouvelle génération de création de sens n’est pas à l’horizo
>
> c'est urgent.

Machine Translated by Google

De plus, la CI a besoin de systèmes évolutifs dotés d'une puissance de calcul
plus importante que jamais pour traiter les données et fournir des informations aux décideurs
politiques et aux combattants. Dans le cas contraire, les systèmes manuels actuels ne
permettant aux équipes d'analyser qu'une quantité limitée de données à la fois, des
renseignements restent disponibles, alors que ces renseignements pourraient s'avérer
décisifs en cas de crise ou de conflit.
Imaginez alors l'importance, pour la sécurité nationale, d'avoir des algorithmes capables
d'analyser de vastes quantités de données et d'alerter avec précision les scientifiques sur
les informations susceptibles d'intéresser des recherches plus approfondies.

Mais ce n'est pas seulement une question de technologie. Ce qu'il faut, c'est
modernisation complète de l'entreprise, y compris
stratégie, gouvernance, culture, talents, données, technologies et processus
informatiques. À cette fin, le Conseil d'innovation de la défense a recommandé
d'« aligner les incitations pour accélérer l'adoption des technologies » en prenant en
compte les risques, en fournissant une « protection optimale » et en mettant fin à
la tendance à récompenser la médiocrité, accélérer l'innovation et le développement
technologique, créer un cheminement de carrière pour les innovateurs, suivre les niveaux
de préparation à l'innovation des personnes, définir une vision pour
l'innovation et la création d'une culture d'apprentissage et d'innovation.

En misant sur l'innovation axée sur la mission, votre organisation peut non seulement
se concentrer sur l'acquisition rapide des dernières technologies, mais aussi sur
l'accélération des résultats de sa mission. Vous pouvez adopter plus rapidement les
technologies clés répondant aux besoins actuels et futurs, et maximiser la probabilité
que les investissements conduisent à la mise en place de capacités adaptées et
efficaces.
à la vitesse de la mission, tenez compte du savoir-faire et du flux de travail
prendre en compte dès le départ, envisager de manière proactive la capacité
d'évoluer au fil du temps et de répondre aux besoins de traitement futurs,
et atténuer le risque que les capacités déployées deviennent
rapidement obsolètes.

Le Conseil d'innovation de la Défense a appelé à une meilleure
compréhension du fonctionnement de l'industrie, à un sens des
affaires accru et à une collaboration plus étroite avec les fournisseurs de
technologies de pointe. Des partenaires industriels qui apportent une
compréhension approfondie des missions et des relations clés avec d'autres leaders.
fournisseurs de technologies cruciales, par exemple le cloud computing,
L'IA et le ML peuvent permettre au CI de créer des systèmes plus résilients et
une création de sens réactive à grande échelle. Imaginez, par exemple,
intégrer des centaines de nouveaux modèles pour augmenter et améliorer
métier, offrant un avantage évident aux décideurs politiques ainsi qu'au personnel
sur le terrain.

Le besoin d'une nouvelle génération de création de sens n'est pas révolu.
horizon — il y a urgence. Bill Burns, alors directeur de la CIA, a déclaré
bien ou à quel point l'agence exploite mal les technologies émergentes et
transforme son métier – pour garder une longueur d'avance sur ses adversaires –
« fera ou détruira notre service de renseignement professionnel ».
Il en va de même pour le CI dans son ensemble. Il est temps d'agir.

Ensemble, le CI et l'industrie peuvent relever ce défi.
Pour commencer à créer dès aujourd'hui des systèmes de création de sens de nouvelle génération,
Votre organisation peut prendre les trois mesures suivantes.

1. Avance

> Évaluez votre état actuel et construisez un
feuille de route. Utiliser un cadre holistique qui permet aux
organisations de comprendre, développer et renforcer leurs
capacités d'analyse. Identifier les forces, les
lacunes et
besoins dans de multiples domaines, notamment la
stratégie, la gouvernance, la culture, les talents,
données, technologie et processus informatiques.
Établir des tableaux de bord pour prioriser les axes de
modernisation. Élaborer et diffuser une vision stratégique
de modernisation. Inclure des objectifs et des réussites
clairement définis et réalisables.
métriques. Évaluer la maturité des capacités actuelles de
cybersécurité Zero Trust. Construire
une feuille de route de modernisation avec les mesures nécessaires
actions, échéanciers et ressources pour atteindre les objectifs
de modernisation à court et à long terme avec des résultats
mesurables.

> Concentrez-vous sur les données. Les données sont essentielles à la compréhension.
Moderniser la technologie de stockage de données back-end
pour un système hérité pour améliorer les données
gestion, intégration au-delà des cloisons,
l'accessibilité et la disponibilité, et de permettre
Flux de travail ML.

> Activer les opérations ML. Développer les technologies modernes
architecture des données et concepts de maillage de données pour
Mettez en place des pipelines de ML pour la modélisation
prédictive avec évaluation continue. Évaluez les meilleurs
modèles de base pour synthétiser de grandes quantités de
données. Établissez des processus permettant à plusieurs
modèles de choisir l'outil adapté à chaque tâche. Ne mettez
pas tous vos œufs dans le même panier. Soyez prêt à mettre à
jour en permanence.
Un exemple de mesure de réussite serait « atteindre une
disponibilité des données de 98 % ».

> Tirez parti des principaux outils DevOps. Utilisez un
Cadre de déploiement incluant des clusters open source pour
l'hébergement de logiciels conteneurisés. Mise en place d'un
développement basé sur l'IA.
environnements avec des pipelines de déploiement continu de
faible à élevé pour augmenter la vélocité
et l'agilité. Inclure la santé du programme
suivi et mesures.

> Exploiter le développement humain. Appliquer une approche centrée sur l'humain.
principes de conception (HCD) pour comprendre comment
Les solutions Verify s'intègrent aux flux de travail des
analystes du renseignement. Elles complètent et améliorent
les flux de travail existants.

Machine Translated by Google

3 étapes pour créer la prochaine génération Systèmes de création de sens maintenant

2. Activer

> Mener des projets pilotes de modernisation. Inclure des activités de gestion du changement. Optimiser la compréhension, la volonté et la capacité des effectifs à passer de la situation actuelle à la situation future est crucial pour la gestion des risques. Identifier un système ou un processus pour la modernisation. Commencer par un système à échelle limitée et non critique.

> Lancer la modernisation. Mener des activités de modernisation sur le système/processus sélectionné. Aligner les critères de réussite sur les impacts réels de la mission, en se concentrant non pas sur la technologie, mais sur ce qu'elle permet. Privilégier la livraison itérative et l'intégration à la mission. Mettre en avant les résultats de la mission et les impacts mesurables pour les principales parties prenantes.
Formez et impliquez les utilisateurs. Documentez les nouvelles pratiques et les nouveaux flux de travail. En vous appuyant sur l'évaluation précédente, adoptez des fonctionnalités Zero Trust pour favoriser une sécurité centrée sur les données, le partage des données entre les enclaves de sécurité et une meilleure interopérabilité. Partagez les résultats avec les principales parties prenantes. Si, par exemple, vous réussissez à moderniser votre infrastructure pour réaliser des analyses avancées à grande échelle, la direction sera probablement intéressée.

> Introduire des assistants numériques. L'introduction d'assistants numériques dotés d'IA pour optimiser la productivité des analystes est un exemple d'activités de modernisation potentielles.
Intégrez-les dans des environnements de travail et des flux de travail communs pour intégrer de manière proactive des recherches applicables et fournir une analyse préliminaire afin que les humains puissent se concentrer sur des activités à plus forte valeur ajoutée.

3. Accélérer

> Efforts de modernisation à grande échelle. Moderniser les systèmes et infrastructures critiques de manière itérative. Mesurer et surveiller les performances et les optimiser. Développer la documentation et favoriser le partage des connaissances.
Normaliser les savoir-faire et les flux de travail pour accomplir la mission dans toute l'organisation.
Poursuivez l'engagement des utilisateurs, les retours et les activités d'intégration. Maintenez une communication claire et cohérente à toutes les phases et gérez les attentes.
Soyez prêt à adapter la feuille de route en fonction des nouvelles connaissances et à gérer et atténuer les risques.

> Développer des fonctionnalités d'agent IA. Voici un exemple de modernisation évolutive. Prototyper et commencer à déployer progressivement des fonctionnalités d'agent IA capables de…
avec supervision : complétez les flux de travail de renseignement de routine en interagissant avec les bases de connaissances, les outils et les systèmes externes pour augmenter de manière significative la productivité, l'efficacité et le temps nécessaire pour obtenir des informations.

Don Polaski est un leader du secteur de la sécurité nationale de Booz Allen, axé sur le développement de solutions d'IA et de science des données qui génèrent des résultats de mission à grande vitesse et à grande échelle.

Marissa Beall est une scientifique des données qui se concentre sur l'application de l'IA et des analyses avancées multi-INT pour transformer les missions de sécurité nationale et le savoir-faire commercial.

Christopher Castelli est responsable de l'engagement sectoriel Zero Trust au sein de l'activité National Cyber de Booz Allen, axée sur les défis et les solutions de sécurité.

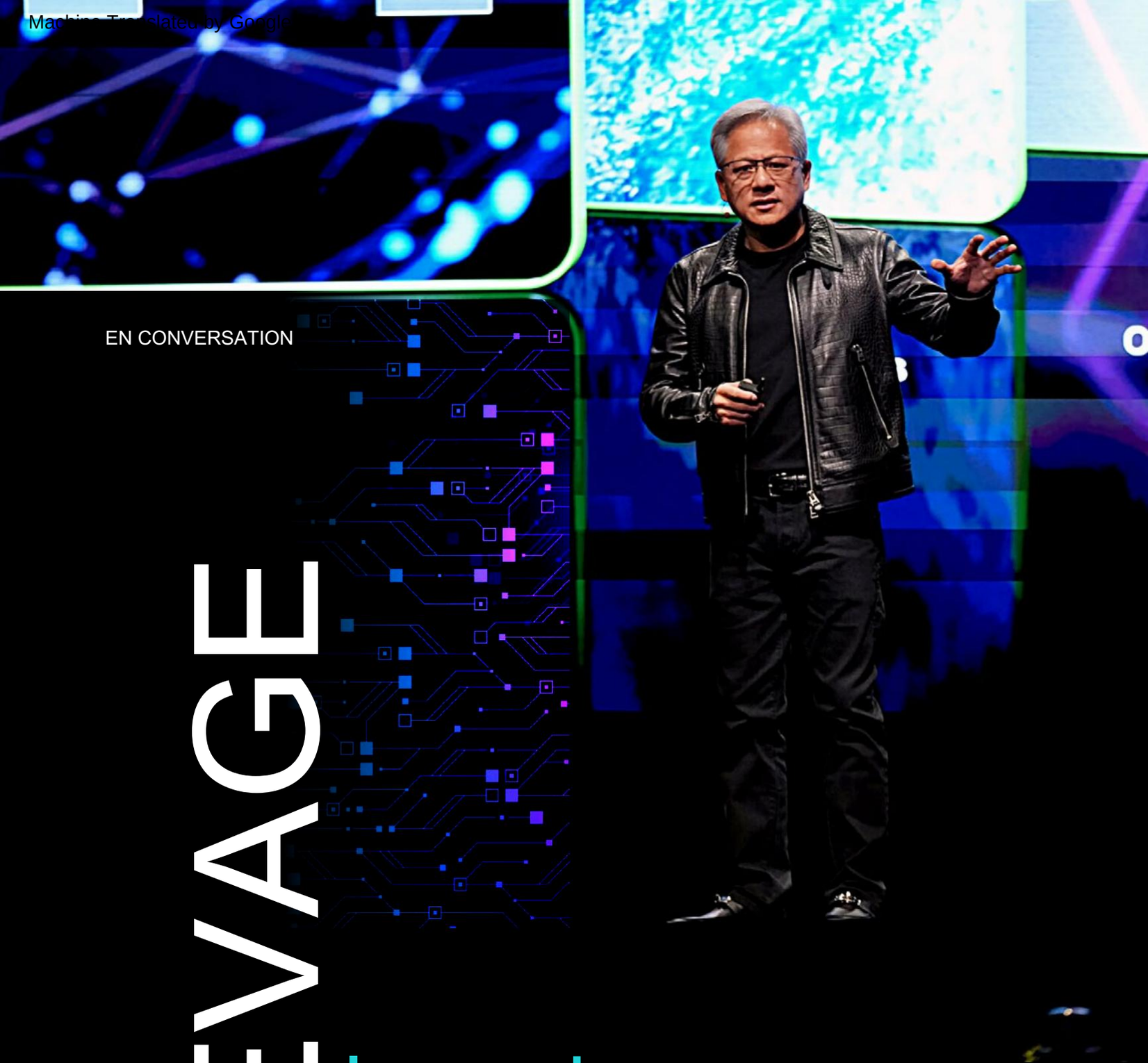
LECTURE RAPIDE

Pour répondre aux défis urgents en matière de sécurité nationale dans le monde, les analystes et les combattants de la communauté du renseignement (CI) doivent donner un sens à des situations complexes et incertaines. Pour ce faire, ils ont besoin de systèmes de compréhension de nouvelle génération capables de collecter et d'analyser des données à une échelle exponentiellement croissante.

Ces outils peuvent synthétiser rapidement les données, présenter des options aux analystes et servir d'assistants. Imaginez, par exemple, de nouveaux algorithmes conçus pour renforcer la collecte, des capteurs plus puissants dotés d'une plus grande puissance d'analyse en périphérie, des modèles de vision par ordinateur pour capturer de nouveaux objets ou détecter des changements dans des zones clés, des agents de modèles de langage volumineux (LLM) facilitant le tri de volumes massifs de données, et des services d'analyse combinant signaux commerciaux et imagerie satellite.

Il est temps d'agir. Les organisations peuvent dès maintenant créer des systèmes de création de sens de nouvelle génération en évaluant l'état actuel et en établissant une feuille de route, en lançant des projets pilotes de modernisation et en accélérant la modernisation à grande échelle.

Machine Translated by Google



EN CONVERSATION

ÉLEVAGE

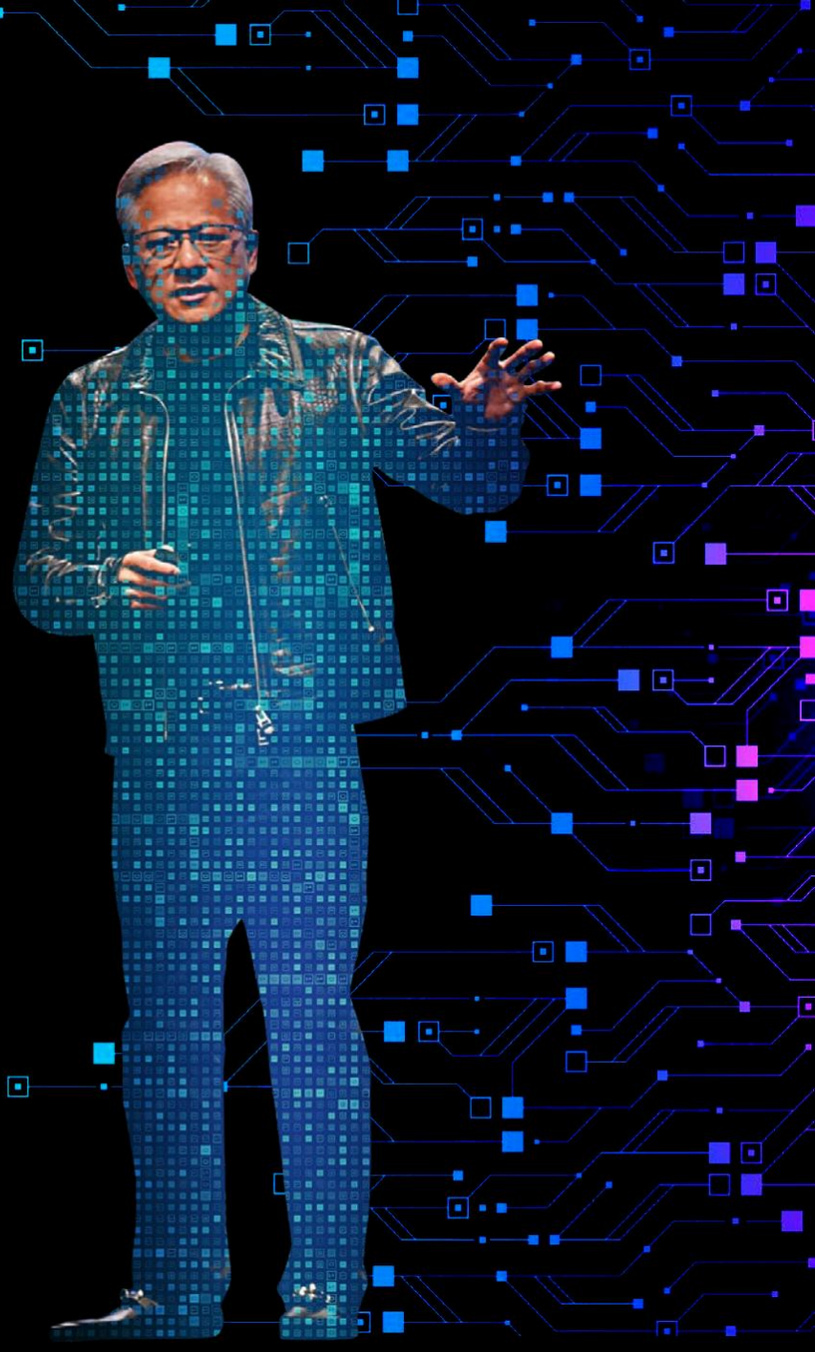
les enjeux pour Accéléré Informatique

Une conversation avec Jensen Huang, fondateur et PDG de NVIDIA

Le calcul accéléré et l'intelligence artificielle générative (GenAI) sont les technologies les plus transformatrices de notre époque. Elles permettent aux dirigeants d'agences fédérales et d'entreprises privées de repenser la manière dont ils relèvent les plus grands défis de leurs organisations. Alors que ces technologies continuent d'évoluer et de développer leurs capacités, la question qui préoccupe les dirigeants du monde entier est : « Que nous permettra l'IA de faire ensuite ? »

Fondateur et PDG de NVIDIA, Jensen Huang est l'un des pionniers de la révolution de l'IA. Les plateformes de calcul de NVIDIA sont à la pointe du calcul accéléré, propulsant un large éventail d'applications dans tous les secteurs. NVIDIA innove également dans d'autres domaines clés, tels que le calcul haute performance, les réseaux, la robotique et les jumeaux numériques physiquement précis.

Nous avons discuté avec Jensen de l'avenir des grands modèles linguistiques (LLM), des raisons pour lesquelles le gouvernement fédéral doit devenir un praticien de l'IA et des raisons pour lesquelles persévérer dans la douleur fait partie intégrante de la réalisation d'une véritable innovation dans n'importe quel domaine.



Q Vous avez fondé et dirigez maintenant une entreprise au centre de la révolution de l'IA. Qu'est-ce qui vous enthousiasme le plus dans la prochaine ère de l'informatique ?

UN Pour la première fois, l'ordinateur est passé du statut d'outil à celui de générateur d'intelligence et de compétences. Nous entrons dans une ère où les ordinateurs ne se contentent plus de traiter des données, mais créent de nouvelles connaissances, résolvent des problèmes complexes et améliorent les capacités humaines comme jamais auparavant. Grâce au calcul accéléré et à l'IA, nous construisons des machines capables de comprendre et de raisonner ; votre ordinateur générera désormais activement des compétences et exécutera des tâches.

Ces usines d'IA génèrent des jetons d'intelligence à grande échelle, transformant les industries par un apprentissage, un raisonnement et une évolution continus. Les ordinateurs deviennent une force dynamique et continue, produisant de l'intelligence en permanence, que nous interagissions avec eux ou non.

Ce changement représente une transformation fondamentale de l'informatique, où l'IA devient un collaborateur, un assistant, et même un créateur aux côtés des humains. Elle inaugure une nouvelle révolution industrielle, stimulant l'innovation dans tous les secteurs. Tout cela est aujourd'hui à notre portée, et les possibilités sont infinies. Qu'il s'agisse de simuler la météo pour éclairer les politiques climatiques, d'accélérer la découverte de médicaments pour des traitements plus rapides ou d'améliorer la cybersécurité grâce au traitement des données en temps réel, l'IA stimule l'innovation dans tous les secteurs tout en étant plus économe en énergie.

Q NVIDIA réinvente l'ensemble de l'environnement informatique, et il y a un concept que vous appelez le « système à trois ordinateurs » problème. » À travers cette idée, quelle est votre vision de l'informatique ?

UN Décomposons cela en deux éléments pour mieux comprendre le problème et l'opportunité.

La première étape, et la plus importante, consiste à créer un écosystème où l'IA deviendra partie intégrante de notre monde, intégrant harmonieusement les sphères numérique et physique. La deuxième étape, que nous appellerons le « problème des trois ordinateurs », décrit comment nous apportons la nouvelle vague d'IA, que nous décrivons comme

« IA physique », à la vie au sein de cet écosystème. Cette triade de puissance de calcul – une pour créer, une pour simuler et une pour exécuter l'IA – représente un changement fondamental dans notre approche de la résolution de problèmes et de l'innovation.

Le premier ordinateur est le système de formation et d'inférence de l'IA. C'est ici que des modèles d'IA massifs sont développés et entraînés grâce au calcul accéléré. Ces modèles sont ensuite déployés pour l'inférence en temps réel dans divers secteurs, pilotant ainsi des applications allant des modèles linguistiques aux systèmes autonomes. Cela fait partie de notre plateforme DGX.
Ensemble, ces solutions facilitent le déploiement de l'IA pour les organisations. Par exemple, des entreprises comme ServiceNow utilisent NVIDIA NIM avec leurs clients fédéraux pour créer de meilleurs systèmes de gestion interne.

Le deuxième ordinateur est l'environnement de simulation, que nous appelons NVIDIA Omniverse. Dans Omniverse, nous simulons des mondes physiques avec une précision inégalée, ce qui nous permet de concevoir, tester et entraîner l'IA dans des répliques virtuelles du monde réel. Cela nous permet de simuler des systèmes complexes, des véhicules autonomes aux robots d'usine, dans des jumeaux numériques qui reproduisent parfaitement les environnements physiques. Ceci est essentiel pour la sécurité, l'efficacité et l'évolutivité, permettant de tester l'IA dans des mondes virtuels avant d'interagir avec le monde physique.

Le troisième ordinateur est l'appareil périphérique, qui pourrait être notre plateforme Jetson ou des ordinateurs portables et stations de travail NVIDIA RTX, où l'IA rencontre le monde réel. Ces machines autonomes, telles que les robots, les drones, les voitures sans conducteur, etc., fonctionnent dans le monde physique grâce aux modèles d'IA entraînés sur le premier ordinateur et testés dans les environnements simulés du second.

Q Dans les conversations sur l'IA, le gouvernement fédéral

Ce n'est généralement pas la première chose à laquelle on pense. Pourtant, l'IA est intégrée à certaines des missions les plus cruciales de notre pays, dans de nombreux domaines, plus significativement que dans le secteur privé. Quel est, selon vous, l'avenir des innovateurs fédéraux qui exploitent l'IA dans des environnements à haut risque ?

UN Le gouvernement fédéral a toujours été un pionnier dans les tests et même dans la création de technologies. Les agences fédérales ont l'opportunité unique de définir la norme en matière d'IA dans les environnements à haut risque. La prochaine étape consiste à faire évoluer l'IA pour prendre des décisions plus rapides et plus précises, tout en garantissant la transparence, la sécurité et la responsabilité de ces systèmes.

La cybersécurité est un autre domaine crucial. Le plan d'action NVIDIA NIM Agent pour la sécurité des conteneurs offre aux entreprises un outil puissant pour protéger leurs infrastructures critiques grâce à la détection et à l'analyse des menaces en temps réel. C'est vraiment incroyable. Ce plan peut aider les développeurs en cybersécurité à réduire les délais de réponse aux menaces de quelques jours à quelques secondes, un véritable bond en avant pour la sécurité.

La convergence de l'IA, du calcul accéléré et de la simulation, comme les jumeaux numériques, est déjà à l'œuvre, mais deviendra de plus en plus importante dans les environnements à haut risque. En simulant des environnements comme les environnements régionaux, Qu'il s'agisse de climats ou d'infrastructures critiques, les agences peuvent tester en toute sécurité les systèmes d'IA avant de les déployer en situation réelle. Cela contribue à réduire les risques et à accroître la fiabilité.

Un parfait exemple est l'annonce faite lors de notre Sommet sur l'IA à Washington, DC, avec MITRE et Mcity de l'Université du Michigan. Ces deux organisations utilisent NVIDIA Omniverse pour valider en toute sécurité des systèmes autonomes dans des environnements virtuels et physiques. En créant un banc d'essai numérique reproductible et reproductible pour les environnements critiques, les innovateurs fédéraux peuvent accélérer l'innovation tout en garantissant la sécurité avant le déploiement en situation réelle.

Q Il est urgent que les agences fédérales accélèrent l'adoption de l'IA. Quels sont les obstacles qui freinent l'intégration rapide de l'IA dans leurs missions essentielles ?

UN Premièrement, chaque agence du gouvernement américain doit devenir un praticien de l'IA, et pas seulement un gouverneur de l'IA. Nous allons devoir utiliser l'IA pour tous les travaux essentiels à la mission, y compris la création de nouveaux algorithmes d'IA pour faire progresser notre pays.

Deuxièmement, nous devons renforcer les infrastructures nécessaires pour soutenir pleinement l'IA. Les États-Unis devraient être le plus grand investisseur mondial dans l'IA ; nous ne pouvons pas nous permettre de ne pas l'être. Les États-Unis devraient construire un supercalculateur pour mener à bien leurs projets ambitieux, comme la découverte d'un remède contre le cancer. Nous collaborons avec de nombreux pays pour développer leur infrastructure souveraine d'IA et leurs supercalculateurs. Au Royaume-Uni, nous disposons de Cambridge-1, un supercalculateur d'IA qui accélère la recherche en santé et en sciences de la vie, aidant ainsi les entreprises pharmaceutiques et les instituts de recherche à faire progresser la découverte de médicaments, la génomique et l'imagerie médicale.

Enfin, nous devons faire des États-Unis le pays le plus attractif pour tous les chercheurs en IA. De plus, nous devons faire de la formation et du perfectionnement de notre main-d'œuvre à l'utilisation de l'IA une priorité nationale. Nous devons être des pionniers dans ce domaine. Chaque organisation, en particulier au sein du gouvernement fédéral, sera transformée par l'IA.

Q Que peut faire le secteur privé pour apporter les meilleures technologies et capacités à grande échelle au gouvernement fédéral ?

UN Nous sommes là pour aider le gouvernement fédéral, quels que soient ses besoins. La responsabilité du secteur privé est de contribuer à l'essor, à la formation et à la mise à disposition de notre expertise et de notre innovation pour accompagner le développement de notre gouvernement. Nous collaborons avec de nombreuses agences, telles que les National Institutes of Health (NIH) et la National Oceanic and Atmospheric Administration (NOAA), pour contribuer au déploiement des technologies les plus récentes, qu'il s'agisse de créer un jumeau numérique ou de développer un NIM pour la découverte de protéines. En travaillant ensemble, nous pouvons traduire les avancées en IA, en simulation et en calcul haute performance en applications concrètes qui renforcent la résilience nationale, améliorent la prise de décision et améliorent l'efficacité à tous les niveaux de gouvernement.

« La convergence de l'IA, du calcul accéléré et de la simulation, comme les jumeaux numériques, est déjà en jeu, mais deviendra de plus en plus importante dans les environnements à haut risque. »

Q Au cours des 10 dernières années, la plupart des systèmes informatiques à grande échelle Nous sommes passés à une architecture orientée services et microservices. Aujourd'hui, l'avenir semble se tourner vers une architecture orientée agents, dans laquelle les agents d'IA interagissent et se lient entre eux. Pouvez-vous nous parler de votre vision de l'évolution de cette architecture ?

UN Chez NVIDIA, nous appelons cela « l'IA agentique ». La première utilisation de l'IA générative s'appuie sur les LLM et permet de fournir des résultats en réponse à une demande. Posez-lui une question et elle vous donne une réponse.

La prochaine ère sera celle de l'IA agentique, où les systèmes d'IA pourront analyser de nombreux scénarios, interagir avec d'autres agents IA et même agir en votre nom en fonction des informations dont ils disposent. À l'avenir, elle ressemblera davantage aux employés d'une organisation. L'IA agentique transforme déjà les secteurs d'activité en automatisant des tâches complexes, permettant ainsi aux collaborateurs de se concentrer sur les domaines où ils maximisent leurs talents.

De nombreuses organisations sont enthousiasmées par la puissance de l'IA agentique, mais ont besoin d'aide pour exploiter son potentiel. NVIDIA simplifie et accélère l'IA agentique avec ses partenaires. Ils utilisent NIM Agent Blueprints pour aider leurs clients à créer des systèmes d'IA agentique.
Ces systèmes d'IA agentiques seront un jour capables de fonctionner de manière autonome et de soutenir un comportement d'IA responsable avec une surveillance humaine minimale.

Q On assiste à une course à la création de LLM plus performants, même si certains commencent à remettre en question leur viabilité économique. Que pouvons-nous attendre des LLM à l'avenir ?

UN Nous allons au-delà des interactions textuelles des LLM pour entrer dans l'ère des LLM multimodaux et de l'IA agentique, où les modèles collaboreront pour comprendre et répondre à une combinaison de texte, de parole et d'images. L'IA deviendra ainsi beaucoup plus intuitive et contextualisée. Imaginez pouvoir interroger un modèle non seulement sur un document écrit, mais aussi sur l'analyse et la synthèse d'un graphique, l'interprétation d'un tableau, voire l'interaction avec une image, et laisser l'IA intervenir pour mener à bien les étapes suivantes de votre projet. Cela ouvre des possibilités infinies pour les entreprises de tous les secteurs.

Nous assisterons également à des avancées majeures dans la personnalisation et l'optimisation des LLM. Cette optimisation permet aux entreprises d'adapter ces modèles fondamentaux à leurs besoins spécifiques, de manière sûre et efficace, les rendant ainsi plus applicables aux problématiques du monde réel. Je suis enthousiasmé par les possibilités offertes par les garde-fous, indispensables à notre protection.

Je ne serais pas surpris si nous avions de nombreuses applications d'IA qui se contrôlent mutuellement et se tiennent mutuellement responsables.

Tout cela est rendu possible par ce que nous appelons la génération augmentée par récupération (RAG). La RAG rend l'IA générative plus précise, car elle extrait des données réelles pour les modèles en temps réel, ce qui rend les résultats plus pertinents et précis, sans nécessiter de réentraînement constant des modèles. C'est une révolution pour les entreprises qui souhaitent intégrer l'IA à leurs flux de travail.

L'avenir des LLM ne se résume pas seulement à la taille ou à l'échelle. Il s'agit de polyvalence, de précision et d'intégration. Nous verrons les modèles faire progresser la recherche et évoluer vers des modèles de langage spécialisés pour des tâches de niche, aidant les entreprises à résoudre des problèmes complexes de manière sécurisée et personnalisable. L'IA devient rapidement un outil crucial dans tous les secteurs, et ces modèles volumineux et spécialisés sont essentiels pour la prochaine vague d'IA.

Q Si vous vous asseyiez aujourd'hui avec un étudiant en ingénierie ou un groupe de stagiaires d'été chez NVIDIA, que leur diriez-vous ?

UN Je dis à cette génération qu'elle participe à l'une des plus grandes mutations technologiques depuis le lancement du System/360 par IBM il y a plus de 60 ans. Le travail qui l'attend est ambitieux et incroyablement important, car il n'a jamais été réalisé auparavant. Les travaux qu'ils choisiront d'entreprendre redéfiniront les industries et façonneront l'avenir de l'humanité. L'IA, le calcul accéléré, la robotique et la simulation révolutionneront tout, de la santé à la science du climat.

Rien de tout cela ne sera facile, mais rien de valable ne l'est jamais. Persévérer malgré la douleur et la souffrance fait partie du chemin. Chez NVIDIA, nous avons connu de nombreux revers et échecs. Grâce à cela, nous sommes devenus extrêmement résilients et sommes une meilleure entreprise grâce à tous les échecs que nous avons surmontés.

Jensen Huang a fondé NVIDIA en 1993 et occupe depuis sa création les fonctions de président-directeur général et de membre du conseil d'administration. Élu à la National Academy of Engineering, il a reçu la plus haute distinction de la Semiconductor Industry Association : le prix Robert N. Noyce ; la médaille des fondateurs de l'IEEE ; le prix Dr. Morris Chang pour leadership exemplaire ; et des doctorats honorifiques de l'université nationale Chiao Tung, de l'université nationale de Taiwan et de l'université d'État de l'Oregon. Il est titulaire d'une licence en génie électrique de l'université d'État de l'Oregon et d'un master en génie électrique de Stanford.

Machine Translated by Google

TECH À COMPLET VITESSE

Le volant d'inertie moderne
Effet expliqué

Bill Vass

L'intelligence artificielle (IA), de l'apprentissage automatique traditionnel (ML) à l'IA générative (GenAI), est un formidable accélérateur grâce à sa polyvalence. Elle peut accroître la productivité humaine en automatisant des tâches répétitives qui, autrement, demanderaient un temps et des efforts précieux. Elle peut ingérer des données et les exploiter pour renforcer continuellement ses capacités. Plus important encore, elle peut optimiser les performances d'autres technologies.

Dans l'article « AI& Everything », paru dans le deuxième numéro de Velocity, le président et directeur général de Booz Allen, Horacio Rozanski, a souligné à juste titre que le véritable potentiel de l'IA sera libéré lorsqu'elle sera associée à d'autres technologies pour générer des résultats transformationnels. Cet avenir souhaité est désormais à portée de main. La convergence des logiciels et du matériel permet de créer des écosystèmes intelligents qui permettent aux agences fédérales d'exploiter pleinement le potentiel de l'IA et d'autres technologies.

Digitized by Google

Machine Translated by Google

Un guide sur les jumeaux numériques

Un jumeau numérique logique se concentre sur les aspects fonctionnels et comportementaux du logiciel et de la logique de contrôle d'un système physique plutôt que sur ses propriétés physiques. Il reproduit les processus décisionnels, les algorithmes et les flux de travail pour permettre la simulation, l'analyse et l'optimisation des opérations. Imaginez un jumeau numérique de la logique opérationnelle d'un réseau intelligent, qui modélise la distribution et l'optimisation de l'électricité en fonction des tendances de la demande. En modélisant les composants logiques, ce type de jumeau numérique permet aux développeurs et aux ingénieurs de tester les mises à jour logicielles, les stratégies de contrôle et les intégrations de systèmes dans un environnement virtuel sans risque. Il est possible et conseillé de créer des jumeaux numériques logiques d'environnements définis par logiciel, tels que les systèmes de planification des ressources de l'entreprise, et de systèmes composés de composants physiques et de technologies opérationnelles (OT).

Un jumeau numérique de processus modélise les processus opérationnels d'un système physique ou d'un flux de travail. Il simule la séquence d'actions, d'interactions et de transformations au sein d'un processus, permettant ainsi un suivi, une analyse et une optimisation en temps réel.

Imaginez un jumeau numérique d'une chaîne de montage simulant l'interaction entre les machines, les ouvriers et les matériaux. En reproduisant le comportement du processus réel, ce type de jumeau numérique permet aux ingénieurs et aux opérateurs de prédire les résultats, d'identifier les inefficacités et de tester les modifications.

Un jumeau structurel 3D modélise la géométrie physique et les caractéristiques structurelles d'un objet ou d'un système réel en trois dimensions. Il capture des informations détaillées sur la forme, les matériaux et les propriétés mécaniques de l'objet ou du système, permettant ainsi la simulation et l'analyse du comportement structurel dans diverses conditions. En fournissant un environnement virtuel pour tester les contraintes, les déformations, la capacité portante et d'autres interactions physiques, un jumeau structurel 3D permet aux ingénieurs et aux concepteurs de prédire les performances, d'optimiser les conceptions et d'identifier les problèmes potentiels avant qu'ils ne surviennent dans le modèle physique. Imaginez un jumeau numérique d'un pont, simulant les contraintes dans diverses conditions pour prédire les besoins de maintenance.

L'infrastructure pour alimenter l'IA

Au début de ma carrière, j'ai travaillé sur un programme qui s'efforçait d'utiliser les réseaux neuronaux pour apprendre aux sous-marins autonomes de la toute première génération à naviguer seuls. Ce projet n'a pas atteint son objectif, mais il m'a permis de comprendre un point important concernant l'IA. Les mathématiques vectorielles et scalaires fondamentales que nous utilisions pour le réseau neuronal de navigation étaient fondamentalement les mêmes que celles qui fondent les systèmes d'IA actuels. Ce qui nous manquait, c'était la capacité de stockage de données et la puissance de calcul nécessaires pour former correctement les réseaux neuronaux afin d'obtenir les résultats souhaités.

Aujourd'hui, la puissance de calcul et les capacités de stockage des données dont disposent les agences fédérales sont exponentiellement plus importantes, et les avancées de l'IA de génération ont ouvert de nouvelles voies d'innovation. Pour revenir au défi des machines autonomes, la MIT Technology Review de novembre 2024 a publié un article sur la technologie. Il a été rapporté qu'un trio de chercheurs avait utilisé des modèles GenAI et un simulateur physique pour apprendre à un chien robot à monter les escaliers et à escalader une boîte sans avoir préalablement entraîné le robot sur des données réelles. C'est un exemple de la façon dont l'IA, intelligemment associée à d'autres technologies, peut révolutionner l'art du possible.

Pour faire évoluer l'IA afin qu'elle puisse être appliquée aux plus grands défis auxquels notre nation est confrontée — De la gestion de la dette nationale à la suprématie technologique de ses concurrents, le gouvernement devrait regarder au-delà des algorithmes et des modèles d'IA et investir dans les infrastructures qui permettront à l'IA de prospérer. Tout comme la construction de réseaux de fibres optiques a contribué à l'essor d'Internet, les mesures suivantes permettront aux agences d'exploiter pleinement le potentiel de l'IA.

- Prioriser les données : connecter tous les réseaux et appareils de l'entreprise (par exemple, les satellites, (drones) pour collecter et stocker autant de données OT que possible. De plus, commencez augmentant le volume de données informatiques enregistrées. Les données OT et IT peuvent et doivent être utilisées pour la formation et la simulation de modèles d'IA. Plus les données que vous fournissez à un modèle sont claires et pertinentes, plus ses ensembles de paramètres sont denses sera, ce qui augmentera sa précision et ses capacités.

- Tirer parti des environnements définis par logiciel : appliquer les pratiques d'ingénierie logicielle pour transformer des systèmes dépendants du matériel en systèmes dynamiques définis par logiciel Environnements. Certaines organisations ont utilisé des processus définis par logiciel pour automatiser des tâches complexes dans les systèmes de planification des ressources d'entreprise. Il est désormais temps d'étendre ce concept à tous les aspects des déploiements physiques et virtuels.

- Utiliser des jumeaux numériques : Utilisez des jumeaux numériques pour créer des environnements virtuels réalistes qui peut héberger des simulations et des tests, puis utiliser l'IA pour optimiser les performances de ces systèmes.

Ce paradigme peut être compris comme ce que j'appelle le volant d'inertie technologique moderne. Imaginez une entreprise fluide, où chaque information collectée alimente une machine virtuelle. Cette machine virtuelle utilise des jumeaux numériques pour entraîner des modèles d'IA à travers des milliers, voire des millions de résultats simulés. Elle déploie ensuite ces modèles vers un périphérique ou les renvoie vers le cloud, où ils apprennent des déploiements réels et réinjectent ces informations dans les environnements de données réels et synthétiques. Cette séquence se répète indéfiniment. Chaque tour génère davantage de données pouvant être utilisées pour améliorer l'IA et le logiciel système, et ces nouvelles données optimisent le tour de roue suivant.

En exploitant ce paradigme complexe mais réalisable, les agences gouvernementales peuvent atteindre la flexibilité, l'échelle et l'accélération essentielles pour libérer l'IA et la technologie à pleine vitesse.

Les composants individuels qui pilotent le volant d'inertie – données réelles et synthétiques, environnements définis par logiciel, jumeaux numériques – ont évolué différemment, ce qui explique pourquoi son potentiel exceptionnel n'a été pleinement reconnu que récemment. Ses interdépendances sont également extrêmement complexes. Mais à chaque rotation du volant, les performances s'améliorent et l'entreprise en tire profit : elle gagne en efficacité, en innovation et en vulnérabilité aux perturbations.

Examinons chaque partie du processus.

Machine Translated by Google

Connectez-vous et collectez

Aujourd'hui, de vastes quantités de données OT affluent 24 heures sur 24, des signaux des capteurs de l'Internet des objets (IoT) aux mises à jour de la logistique et de la chaîne d'approvisionnement, le tout transmis, souvent via le Wi-Fi. Il est plus facile que jamais d'utiliser l'échange de données informatisé (EDI) pour intégrer ces diverses sources. De plus, les réseaux privés 5G et LoRaWAN, un réseau basse consommation pour appareils sans fil, offrent une connectivité fluide dans des conditions exigeantes, tandis que les nouveaux systèmes satellitaires offrent des connexions à faible latence et haut débit pour les sites distants en périphérie. Grâce à de telles fonctionnalités, vous pouvez vous connecter et collecter des données en continu partout, de l'exaoctet au zettaoctet. Les systèmes informatiques fonctionnant sur site et dans le cloud génèrent également des flux de données (par exemple, des fichiers journaux) qui sont souvent supprimés trop tôt. Ces données peuvent désormais être sauvegardées à moindre coût et devraient être ajoutées au bassin de données plus vaste pouvant être utilisé pour la simulation, les tests et l'entraînement des modèles d'IA.

Tirez parti du Cloud

Mais que faire de toutes ces informations potentielles ? Grâce au cloud, les entreprises peuvent les stocker indéfiniment et à moindre coût, en complétant les données collectées par des données synthétiques pour combler les lacunes connues ou pour des scénarios non testables en situation réelle. Les unités militaires, par exemple, ne peuvent pas exécuter des milliers de scénarios de combat différents, mais les agences peuvent générer des données classifiées « représentatives » sous forme synthétique pour entraîner des systèmes autonomes au futur champ de bataille. Cette même approche permet aux agences civiles de simuler des scénarios de réponse aux crises, de tester la résilience des infrastructures critiques et d'évaluer l'impact des politiques à grande échelle. Grâce à la fusion de données réelles et synthétiques dans des pipelines, les entreprises peuvent assembler les ensembles de paramètres denses nécessaires à la création de simulations fidèles d'environnements réels.

Investir dans des systèmes définis par logiciel

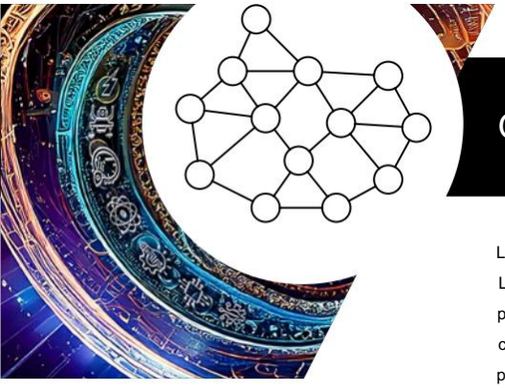
Étant donné que les logiciels continuent de « dévorer » le matériel, les agences qui ne se préoccupent pas suffisamment des environnements logiciels risquent de prendre du retard. L'impératif pour les agences fédérales est de convertir autant de processus et de systèmes d'entreprise que possible en systèmes logiciels. Ce changement permet aux développeurs d'envoyer des mises à jour à distance, ce qui prolonge la durée de vie de leurs systèmes et accroît leur adaptabilité en permettant le déploiement à distance de nouvelles fonctionnalités, de correctifs de sécurité et d'améliorations de performances. De plus, en facilitant le traitement et la connectivité des données en temps réel, les environnements logiciels améliorent les performances et facilitent l'intégration transparente d'algorithmes d'IA et de modèles d'apprentissage automatique, ce qui se traduit par des capacités d'automatisation et de prise de décision intelligentes. Cette approche accélère les cycles d'innovation, réduit les coûts de développement et permet une plus grande personnalisation pour répondre aux divers besoins des utilisateurs, tout en permettant aux systèmes d'apprendre et de s'adapter au fil du temps.

Machine Translated by Google

Simuler et tester

Une fois qu'une agence a optimisé sa définition logicielle, elle peut alimenter le cloud avec ses données réelles et synthétiques et exécuter le système en simulation à l'aide d'un jumeau numérique. Grâce à la puissance de stockage et de traitement du cloud, les organisations peuvent pour la première fois exploiter des jumeaux haute fidélité avec une physique complète et une représentation photoréaliste 3D par lancer de rayons.
Cela combine le jumeau numérique logique, le jumeau numérique de processus et le jumeau structurel 3D en une seule représentation complète, permettant aux organisations d'analyser des scénarios dans un environnement virtuel sans risque.

Les réseaux de jumeaux numériques haute fidélité peuvent modéliser et optimiser des écosystèmes tentaculaires.
Un jumeau numérique d'un réseau électrique, par exemple, pourrait simuler l'impact de diverses politiques énergétiques et des cybermenaces potentielles pour un pays entier. C'est un avantage révolutionnaire qui peut réduire des années de tests à quelques minutes ou permettre le traitement d'un volume massif de combinaisons en quelques heures. Auparavant, il n'existait aucun monde où les unités militaires de première ligne pouvaient simuler de manière réaliste des conditions de combat sans risque pour les combattants et à un coût raisonnable. Aujourd'hui, elles peuvent s'entraîner et s'entraîner au combat.



Optimiser avec l'IA

Les algorithmes ML avancés rassemblent les environnements OT et de simulation en temps réel.
L'apprentissage automatique (ML) combiné au calcul haute performance permet d'analyser des milliards de combinaisons possibles, impossibles à gérer par des moyens humains conventionnels. C'est à ce stade du processus que l'on commence à comprendre comment l'IA apprend des simulations de jumeaux numériques et construit des milliards de paramètres dans le modèle pour son apprentissage.
Les améliorations sont continuellement réinjectées dans le système. Ce processus global crée ensuite les modèles d'IA et de GenAI, qui sont ensuite déployés en production.

Passage à la production

Vous pouvez désormais déployer vos jumeaux numériques en production et les exploiter en périphérie, sur site et dans le cloud. Grâce à des technologies désormais suffisamment matures pour être intégrées et opérationnelles, le volant d'inertie continue d'améliorer les performances de l'entreprise. À mesure que vous collectez davantage de données issues d'opérations virtuelles et réelles, vous pouvez les réinjecter dans le système pour faire tourner le volant d'inertie encore et encore.

Avec un système auto-renouvelable et basé sur l'IA comme celui-ci, le potentiel de transformation des missions essentielles est également illimité. Une agence de défense, par exemple, pourrait utiliser des jumeaux numériques distribués à l'échelle mondiale pour réaliser des simulations de chaîne d'approvisionnement, en intégrant les données des capteurs IoT et l'informatique de pointe afin de tester des scénarios de demande et de se préparer à toute crise créée par ses adversaires.
Pour les organisations gouvernementales chargées de protéger la sécurité nationale, de fournir des services aux citoyens et de gérer les infrastructures critiques, le volant d'inertie moderne offre des avantages uniques qui correspondent aux exigences complexes de leur mission.

AVANTAGES DU VOLANT D'INERTIE MODERNE

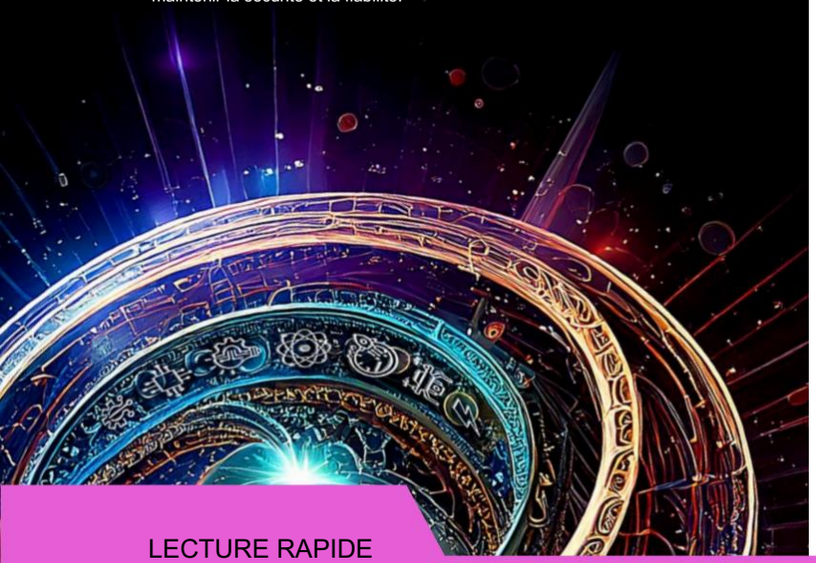
Le volant d’inertie technologique moderne combine des données réelles et synthétiques, des environnements définis par logiciel, des jumeaux numériques et l’IA/ML pour produire des avantages au niveau de l’entreprise.

Modularité et flexibilité
Sépare la dépendance rigide à l'infrastructure matérielle en créant des systèmes d'IA qui peuvent être adaptés, mis à niveau ou optimisés via des couches logicielles, permettant aux modèles d'IA d'être facilement mis à jour ou reconfigurés sans nécessiter de modifications matérielles spécifiques et coûteuses.

Amélioration continue
Fournit aux modèles d'IA des flux de nouvelles données à partir desquels apprendre afin qu'ils puissent évoluer en permanence, en restant alignés sur les dernières avancées et demandes.

Harmonie Edge-to-Cloud : permet aux modèles d'IA d'effectuer des inférences en temps réel en périphérie (par exemple, dans les satellites ou les objets connectés) tout en déchargeant les tâches d'apprentissage plus lourdes sur les systèmes cloud. Cette approche harmonisée garantit une prise de décision rapide et réactive, ainsi que la capacité de traiter des ensembles de données plus volumineux dans des emplacements puissants et centralisés.

Améliorations de la sécurité et de la sûreté Fournit les mises à jour dynamiques nécessaires pour garantir la robustesse contre les nouvelles menaces, biais ou vulnérabilités.
Alors que l’IA est déployée dans des applications critiques, telles que les véhicules autonomes ou la sécurité nationale, la capacité à corriger et à améliorer les systèmes d’IA via des logiciels devient essentielle pour maintenir la sécurité et la fiabilité.



Voler vers l'avenir Pour exploiter les avantages du volant d'inertie moderne, il est essentiel de poser les bases adéquates. Ces bases commencent par les données, qui sont le moteur de l'IA et des jumeaux numériques. Les agences disposant d'ensembles de données plus spécialisés seront mieux placées pour créer des simulations réalistes d'environnements de mission et, peut-être un jour, pour construire leurs propres modèles d'IA. De plus, les actifs logiciels de toutes tailles et de toutes échelles, des réseaux aux navires de guerre, permettent la construction de systèmes adaptables, mis à niveau ou optimisés via des couches logicielles sans nécessiter de modifications matérielles spécifiques et coûteuses. Il est également essentiel d'investir dans la sécurité. Les systèmes connectés introduisent de nouveaux vecteurs d'attaque ; c'est pourquoi les agences doivent utiliser un chiffrement multicouche et des pare-feu complets. L'évolutivité doit être assurée par de multiples zones de disponibilité physiquement séparées, avec un ensemble unifié d'interfaces de programmation d'applications (API) de la périphérie au cloud. Compte tenu de la rapidité et de l'ampleur des cyberattaques, l'IA jouera un rôle essentiel dans l'identification des menaces, la surveillance des vecteurs d'attaque et la chasse proactive aux menaces.

Grâce à ces niveaux de soutien, les agences fédérales sont en mesure d'utiliser le volant d'inertie moderne pour aider l'IA à atteindre plus rapidement les résultats essentiels à leur mission. Pour innover au XXIe siècle, il faut plus qu'un simple ensemble d'outils technologiques disparates. Adapter une application d'IA traditionnelle à un cas d'usage restreint ne suffit plus. Il s'agit désormais d'intégrer plusieurs systèmes modernes basés sur l'IA pour créer une source d'amélioration continue et auto-renouvelable.

La combinaison des technologies émergentes dans les phases de collecte de données, de simulation, de formation et de déploiement constitue la clé pour réaliser des progrès exponentiels en termes d’efficacité, d’innovation et de réussite des missions.

Alors que la réussite des missions a souvent des implications nationales, cette intégration technologique ne se limite pas à une question d'efficacité : elle vise à maintenir un avantage stratégique et à assurer la continuité des services essentiels. L'approche moderne du volant d'inertie permet aux organisations fédérales de s'adapter rapidement aux menaces émergentes, d'adapter leurs services aux besoins des citoyens et de maintenir leur supériorité technologique dans un environnement mondial complexe.

Bill Vass est le directeur technique de Booz Allen. Il a auparavant occupé le poste de vice-président de l'ingénierie chez Amazon Web Services et a été Senior Executive Service (SES) au ministère de la Défense des États-Unis.

LECTURE RAPIDE

Pour innover au XXIe siècle, le gouvernement fédéral doit aller au-delà de la simple adaptation d'une application d'IA traditionnelle à un cas d'usage précis. Les agences doivent plutôt investir dans l'intégration de multiples systèmes modernes d'IA capables d'exploiter pleinement le potentiel de l'IA et d'autres technologies.

Pour construire ces systèmes intelligents, les agences doivent collecter et stocker autant de données technologiques opérationnelles et informatiques que possible, convertir les processus dépendant du matériel en environnements contrôlés par logiciel et investir dans des jumeaux numériques.

Ce paradigme technique réalisable permettra aux organisations fédérales de s’adapter rapidement aux menaces émergentes, d’adapter les services pour répondre aux besoins des citoyens et de maintenir leur supériorité technologique dans un environnement mondial complexe.

Machine Translated by Google

Dans l'apprentissage de l'IA,
Taille unique

Une conversation entre Kian Katanforoosh, Joe Rohner et Jim Hemgen

Le sujet de la préparation à l'intelligence artificielle (IA) est désormais un incontournable, des couloirs du Congrès aux tables rondes de Davos. Il est universellement admis que le chemin à parcourir passe par la mise à niveau, la reconversion et la gestion du changement, notamment pour les 60 % d'emplois des économies avancées qui, selon une étude du Fonds monétaire international , seront affectés par l'IA. Mais ce que nous savons tous à l'échelle mondiale n'apporte guère de clarté à l'individu : l'employé, le candidat ou le dirigeant qui doit tracer son propre chemin.

Kian Katanforoosh est au cœur de ce défi, innovant. PDG et fondateur de Workera, il dirige une équipe qui développe des solutions d'apprentissage par l'IA intelligentes et concrètes, adaptées aux objectifs, aux compétences et aux lacunes de chacun. Joe Rohner, vice-président de Booz Allen et leader de notre activité IA, et Jim Hemgen, directeur du développement des talents de l'entreprise, ont rencontré Kian pour l'interroger sur les perspectives d'avenir en matière de formation et de transformation de l'IA, et sur les moyens d'accélérer ce processus.

Machine Translated by Google

Q Dans votre travail, vous dirigez une entreprise de perfectionnement en IA et Enseigner aux étudiants universitaires. Vous passez la plupart de vos journées S'engager auprès des futurs travailleurs. Selon vous, qu'est-ce qui change fondamentalement la façon dont les gens apprennent l'IA ?

UN L'une des tendances marquantes que je constate dans mes cours est l'arrivée d'étudiants d'horizons divers pour étudier l'IA. J'enseigne au département d'informatique, mais la plupart de mes étudiants en apprentissage profond ne sont pas des spécialistes en informatique. C'est une nouveauté. Nous avons des étudiants issus du génie mécanique, de la science des matériaux, de l'aéronautique et de la médecine qui souhaitent apprendre à appliquer l'IA à d'autres domaines de manière exceptionnelle. Certains de mes étudiants, issus du secteur de l'énergie, ont suivi cette formation pour développer une solution de maintenance prédictive pour un système de forage.

J'appelle ces apprenants « IA+X » et ils deviennent rapidement les principaux utilisateurs de l'IA, que ce soit dans les universités, les entreprises ou les administrations publiques. Ces personnes IA+X étudient la technologie en lien avec leur domaine d'expertise et viennent avec l'intention de résoudre des problèmes concrets.

Q Alors que les postes de l'IA se sont largement ouverts, il est difficile de Imaginez un parcours type de formation en IA. Quelles sont les implications de l'IA+X pour les universités et les employeurs ?

UN C'est vrai : cette cohorte évolutive d'apprenants en IA bouleverse la façon dont beaucoup d'entre nous avaient l'habitude de penser l'éducation, que ce soit à l'université ou au travail.
Une approche unique où les gens restent assis dans une salle de classe pendant un nombre d'heures déterminé ou suivent un programme standard ne sert pas l'apprentissage de l'IA aujourd'hui.
La technologie évolue si rapidement qu'il existe un engouement compréhensible pour la « demi-vie » des compétences numériques qui se réduit. Nous n'avons même pas encore atteint le point le plus bas, il devient donc moins pratique ou raisonnable de consacrer du temps à des contenus non pertinents.

Par exemple, un ingénieur mécanicien maîtrise l'algèbre linéaire, mais devra peut-être apprendre le codage Python, et un ingénieur électricien comprend la transformée de Fourier, mais devra peut-être apprendre de nouveaux algorithmes basés sur les réseaux neuronaux. Il en va de même pour les responsables de mission et d'entreprise qui n'ont pas le luxe de suivre une formation de 200 heures, mais qui doivent continuellement développer leurs compétences en IA.

Le principal défi aujourd'hui est de déterminer comment prendre des décisions éclairées quant à ce qu'il faut apprendre et à quoi consacrer son temps. C'est pourquoi de nombreuses innovations récentes associent l'apprentissage par IA à des agents capables de vérifier les compétences d'un individu, d'optimiser ses lacunes et de proposer du contenu inédit et adapté à ses objectifs d'apprentissage individualisés.

Et l'impact est tangible. Par exemple, chez Workera, nous avons constaté une multiplication par cinq de la vitesse d'apprentissage grâce aux agents d'IA utilisés pour la vérification des compétences. En intégrant les agents d'IA eux-mêmes au processus de montée en compétences, nous sommes en mesure d'optimiser le processus pour l'apprenant et de lui proposer le contenu adapté à chaque situation.

le bon moment et évitez les éléments que l'utilisateur connaît déjà ou qui ne lui offrent peut-être pas le chemin le plus rapide vers le progrès.

Q Vous avez mentionné la demi-vie des compétences, et pour beaucoup d'entre elles avez avancés dans notre carrière, cela peut être désarmant. Comment Pensez-vous personnellement à la pertinence de vos compétences, notamment dans un domaine comme l'IA ?

UN Nous avons probablement dépassé la génération où quelqu'un peut espérer faire le même travail pendant 30 ans, puis prendre sa retraite.
Mais je tiens à souligner que les experts métiers ne sont pas près de disparaître. Au contraire, la demande d'expertise spécialisée augmentera à mesure que l'IA alimente de nouvelles applications.

Concernant ma carrière, je trouve utile de considérer mon évolution sous la forme d'un T. La ligne horizontale en haut du T représente l'étendue de mes compétences durables : ce sont des compétences qui ont une pertinence à long terme, par exemple les mathématiques et les statistiques que j'ai apprises en grandissant en France. Aujourd'hui encore, ces compétences durables me permettent d'aborder rapidement de nouvelles matières avec assurance.
La ligne verticale du T représente les nombreuses compétences durables que j'ai acquises à des moments précis dans un but d'innovation.

Même si chacune de mes compétences individuelles peut avoir une durée de vie différente, c'est la combinaison de compétences périssables et durables qui me permet de suivre le rythme des progrès.
Donc, pour tous ceux qui s'inquiètent de la longévité de leurs compétences : votre futur vous-même a l'avantage d'avoir un ensemble de compétences plus durables et plus durables, même si la pratique de la technologie évolue.

Q Vous passez beaucoup de temps avec des organisations qui sont Investissant beaucoup dans l'IA. Quelle est la question qui revient le plus souvent lorsque vous discutez avec des dirigeants d'entreprise de la transformation des effectifs ?

UN Les organisations et leurs équipes de direction se concentrent sur la mesure et la compréhension des progrès de la transformation de l'IA.
Mais face à la multitude d'indicateurs possibles, les dirigeants s'interrogent sur la manière d'aborder la mesure de l'entreprise.

Je leur recommande de suivre les progrès dans deux catégories parallèles : les résultats et les compétences.

Par résultats, j'entends les changements majeurs qu'une organisation recherche en investissant dans la transformation de l'IA. Par exemple, ces principaux résultats peuvent inclure une productivité accrue, l'innovation et une utilisation responsable. Lorsqu'une organisation a clairement défini ces résultats, elle peut commencer à suivre les principaux indicateurs :

- Quelles nouvelles capacités avons-nous débloquées grâce à l'IA ? (résultat connexe : productivité)
- Combien de projets disposent d'un système compatible avec l'IA en production ? (résultat connexe : innovation)
- Combien d'alertes ou d'incidents ont été signalés ? (résultat connexe : utilisation responsable)

Machine Translated by Google

> Chez Workera, nous avons constaté une multiplication par cinq de la vitesse d'apprentissage grâce aux agents d'IA utilisés pour la vérification des compétences. En intégrant les agents d'IA eux-mêmes au processus de montée en compétences, nous sommes en mesure d'optimiser le processus pour l'apprenant, de lui proposer le bon contenu au bon moment et d'éviter les contenus qu'il connaît déjà.

Parallèlement aux résultats, les entreprises doivent mesurer la progression des compétences acquises par tous les employés participants. Les compétences sont-elles suffisamment développées pour atteindre les objectifs principaux au fil du temps ? L'organisation dispose-t-elle d'ontologies de compétences adéquates et vérifiables ?
Les employés peuvent-ils obtenir une certification dans des domaines critiques (comme l'IA responsable) et reçoivent-ils un retour sur leur développement ?

Les organisations peuvent vérifier les niveaux de compétences de leurs employés dans des domaines spécifiques, en plus de suivre l'indicateur le plus important pour une organisation axée sur les compétences : leur vitesse d'apprentissage globale. Accroître la vitesse d'apprentissage globale (la rapidité avec laquelle les employés progressent dans l'acquisition d'une nouvelle compétence) peut permettre aux entreprises de rattraper et de surpasser rapidement leurs concurrents. Ce type d'évaluation granulaire des compétences aide les dirigeants à évaluer le niveau de maturité de leur organisation et son évolution vers les compétences de l'entreprise.

Q Une transformation de l'IA d'entreprise nécessite des efforts considérables Changements culturels. Quels conseils donneriez-vous aux organisations qui se lancent dans l'IA ?

UN Mon premier conseil s'adresse aux personnes au sommet.
Dans mon travail, j'ai rencontré des leaders aux parcours d'engagement variés. Certains cadres s'impliquent pleinement dans la formation : ils évaluent leurs compétences, comblent leurs lacunes, obtiennent des badges et des certifications.

et ceux qui ne le savent pas, mais prétendent en savoir plus qu'eux-mêmes ou ne se placent pas aux mêmes niveaux d'exigence que leurs collaborateurs. Lorsque les dirigeants fixent des objectifs élevés pour leur propre développement, les employés constatent que « nous sommes tous sur la même longueur d'onde ». Cet engagement des dirigeants contribue grandement à favoriser une culture positive autour de la transformation de l'IA.

Il est également important de prendre en compte la culture qui entoure l'expérimentation. Certaines organisations considèrent l'IA comme un projet à enjeux élevés et privilégient constamment les projets prioritaires. Mais cette approche finira par se heurter à un obstacle, compte tenu de la complexité et des compétences nécessaires pour faire passer les systèmes d'IA du prototype à la production. Mon conseil est de concentrer initialement l'innovation sur des projets modestes mais visibles.
Pensez simplement au désormais célèbre projet Google Brain visant à détecter les chats dans les vidéos, dirigé à l'époque par Andrew Ng.
Ce projet d'IA ne présentait aucun risque pour la mission de l'entreprise si le système ne fonctionnait pas. Mais les gens adorent les chats, et l'approche du projet basée sur les réseaux neuronaux est devenue très visible.
Cela a finalement accéléré la production de réseaux neuronaux au sein d'autres programmes Google aux enjeux plus importants. J'insiste souvent auprès des organisations sur le fait que ces petits efforts, même s'ils peuvent paraître insignifiants, voire futiles, peuvent inspirer des innovations significatives à long terme.

Q En dehors du monde universitaire et du monde du travail technologique, la plupart des gens n'ont pas d'accès réaliste à une formation avancée en IA.
Quels efforts peuvent contribuer à accroître l'accès à l'IA ?

UN De plus en plus d'organisations et de fondations ouvrent la voie à la maîtrise de l'IA au sein des communautés, notamment du primaire et du secondaire. Des programmes de formation sur le terrain à la Journée nationale de la maîtrise de l'IA, elles préparent les jeunes étudiants aux compétences en IA pour l'université et le monde du travail, et proposent des programmes pour doter les enseignants et les administrateurs des outils nécessaires.

Mais l'accès général à l'IA est un défi à long terme qui ne sera pas résolu. être abordé par n'importe quel acteur de l'écosystème et
Il faut que tout le monde soit à la table. Il nous reste encore du chemin à parcourir. pour s'assurer que les communautés et les populations ne sont pas laissés pour compte. Il suffit de penser au vieillissement de la main-d'œuvre ou à la 20 % des ménages américains n'ont pas accès à Internet : la fracture numérique ne fera que s'élargir à mesure que l'IA commencera à avoir un impact sur tous les aspects de la société.

Nous avons parlé plus tôt du modèle en forme de T pour réfléchir aux compétences durables et périssables. Il est important pour souligner que l'IA deviendra à terme une compétence transversale et durable, l'une de ces compétences historiques puissantes dont la demi-vie sera extrêmement longue. L'IA apparaîtra bientôt dans des descriptions de poste auxquelles vous n'auriez peut-être pas pensé ; nous avons donc tous un rôle à jouer pour éliminer les obstacles.

Je suis ravi de voir les progrès que nous allons continuer à réaliser. en tant qu'industrie. Qu'il s'agisse de collaborer avec organisations non gouvernementales, partenaires communautaires, ou le gouvernement fédéral, ou en offrant une formation gratuite programmes (dont je suis fier que nous proposions chez Workera), de petits efforts contribuent grandement à mettre l'IA entre les mains de plus de personnes. En fin de compte, l'accès ne se résume pas à renforcer la main-d'œuvre de demain : la maîtrise de l'IA sera bientôt un besoin humain fondamental pour naviguer dans le monde, des finances aux soins de santé en passant par les prestations gouvernementales.

Kian Katanforoosh est PDG et fondateur de Workera, une plateforme de veille stratégique qui révolutionne la manière dont les entreprises comprennent, développent et mobilisent les talents. Il est membre fondateur de DeepLearning.AI et conférencier primé à l'Université de Stanford.

Joe Rohner est un leader du bureau de la technologie de Booz Allen, spécialisé dans l'adoption de l'IA, les talents et l'éducation.

Jim Hemgen dirige le développement des talents chez Booz Allen et supervise les initiatives visant à aider l'entreprise à constituer une main-d'œuvre prête pour l'IA.

Machine Translated by Google

L'ère de l'IA agentique

L'INTELLIGENCE DISTRIBUÉE RÉIMAGINÉE

John Larson et Alison Smith

Nous approchons rapidement de la point où les systèmes informatiques distribués seront capables de réfléchir rapidement, de s'adapter aux changements majeurs en quelques secondes et de résoudre silencieusement les problèmes sans intervention humaine. C'est la promesse de l'intelligence artificielle (IA) agentique, un paradigme technologique dans lequel des agents autonomes alimentés par de grands modèles de langage (LLM) pourront bientôt s'organiser et se réorganiser pour exploiter des systèmes et des applications critiques de manière entièrement autonome.

Il ne s'agit pas seulement d'une nouvelle mise à niveau technique : le passage à l'IA agentique promet de redéfinir fondamentalement la manière dont les systèmes informatiques sont construits et dont les logiciels fonctionnent dans le monde réel.

Si la complexité inhabituelle de l'IA agentique peut s'avérer difficile à gérer, son formidable potentiel d'accélération des missions et de disruption industrielle souligne la nécessité pour les organisations de mieux comprendre l'IA qui exerce son pouvoir d'action. Lorsque l'IA peut fonctionner seule pour mettre en œuvre des directives et des stratégies sans sollicitations ni interventions spécifiques, quelles nouvelles possibilités apparaissent, et quels sont les risques et les compromis ?

Introduction aux microservices

Les systèmes distribués remontent aux débuts de l'informatique, lorsque des mécanismes de bas niveau, tels que les appels de socket, géraient la communication entre les différents composants d'un système. Dans ces premiers systèmes, chaque composant devait connaître les identifiants mémoire exacts, ou « adresses », des autres composants avec lesquels il interagissait ; les protocoles de communication étaient donc définis de manière rigide. Ce couplage étroit rendait les systèmes fragiles et difficiles à modifier ou à faire évoluer. À mesure que les applications devenaient plus complexes, toute modification d'un seul composant était devenue impossible. un redéploiement potentiellement nécessaire de l'ensemble du système, entraînant un risque accru de bugs tout en allongeant les cycles de développement.

En réponse aux limites des anciennes méthodes monolithiques de création d'applications, l'architecture microservices a émergé. Ce paradigme décompose les applications en services plus petits, moins couplés, qui peuvent être développés, déployés et mis à l'échelle séparément. Chaque microservice encapsule généralement une fonction métier spécifique et communique avec d'autres services via des interfaces de programmation d'applications (API) bien définies. Cette approche modulaire améliore dans une certaine mesure l'évolutivité et l'agilité, permettant aux équipes d'itérer sur des services individuels sans affecter l'ensemble du système. Cependant, l'architecture microservices présente également des inconvénients majeurs :

- Cela crée un besoin d'expertise spécialisée en orchestration de services et en conteneurisation, à laquelle les organisations peuvent avoir du mal à accéder.
- Cela augmente les frais opérationnels en termes de maintenance de plusieurs services et de fluidification de la communication via les API et les courtiers de messages.
- Cela complique la gestion des données car celles-ci sont réparties sur différents services, ce qui crée des incohérences et ralentit les transactions.
- Cela impose des coûts initiaux élevés lors de la migration vers la nouvelle architecture pour la refactorisation de certaines applications et l'investissement dans l'infrastructure cloud.

La promesse potentielle de l'IA agentique

Avance rapide jusqu'à nos jours et l'essor de l'IA générative (GenAI). L'IA Gen ne possède pas encore de « cerveau » de niveau humain ; elle présente des capacités qui servent souvent de substituts au raisonnement et à la flexibilité humains. Contrairement aux systèmes étroitement couplés qui reposent sur des règles prédéfinies et un contrôle centralisé, les systèmes d'IA agentique utilisent des agents génératifs autonomes ou semi-autonomes capables d'interactions dynamiques en temps réel. Considérez désormais chaque microservice ou application devant interagir avec un autre comme un agent plutôt que comme un simple logiciel.

L'hypothèse émergente – devenant désormais de plus en plus plausible – Ces agents pourront bientôt communiquer entre eux de manière dynamique et flexible, sans s'appuyer sur des interactions fixes et prédéfinies. Historiquement, la rigidité des interactions système fragilisait les applications, les rendant souvent inopérantes face à l'évolution des besoins ou à la complexité accrue. À l'inverse, les agents exploitent le contexte, les expériences passées et le raisonnement pour réagir efficacement aux situations et tâches inattendues ou nouvelles. Cette résilience, comparable à celle des humains, permet aux agents d'agir rapidement et précisément, même dans des environnements incertains ou imprévisibles, sans nécessiter d'instructions détaillées.

Même si un framework de microservices avec des API REST (Representational State Transfer) introduit une certaine souplesse en intégrant l'absence d'état du protocole HTTP (Hypertext Transfer Protocol), il n'empêche pas les grands systèmes logiciels de devenir plus étroitement couplés au fil du temps. À mesure que les grands systèmes logiciels mûrissent et se développent, ils sont confrontés à des exigences qui motivent naturellement un couplage plus étroit, telles que les dépendances implicites, les modèles de données partagés et les fonctionnalités transversales.

Machine Translated by Google

telles que la journalisation et l'authentification ; et la rétrocompatibilité avec le code existant. Avec les agents, la communication est entièrement flexible, ce qui leur permet d'interagir et de s'adapter, d'expérimenter, de tester et d'optimiser de manière autonome, en travaillant à l'innovation sans intervention manuelle ni reprogrammation pour implémenter de nouvelles fonctionnalités ou stratégies de résolution de problèmes.

À quoi pourrait ressembler l'IA agentique

La capacité de l'IA agentique à s'auto-organiser et à s'adapter crée de nouveaux cas d'usage pertinents dans tous les secteurs.

Par exemple, GenAI a évolué, passant d'applications LLM uniques à des systèmes d'agents spécialisés travaillant de concert. Aujourd'hui, les agents ont souvent des rôles distincts, tels que la planification et la répartition des tâches, la recherche d'informations, la révision de contenu ou la production.

optimisation. Ils opèrent généralement dans des cadres orchestrés pour résoudre de manière collaborative des problèmes complexes en plusieurs étapes.

Modèles de conception courants pour les agents

Les systèmes d'IA comprennent :

- Orchestration centralisée des agents : Un orchestrateur gère plusieurs agents spécialisés (LLM ou non-LLM services) qui collaborent pour résoudre des tâches complexes.
- Décomposition des tâches décentralisées et la planification : Le système se brise décomposer des tâches complexes en sous-tâches, en utilisant souvent la capacité du LLM à comprendre et organiser le travail progressivement. Séparément les chaînes d'actions modélisées sont souvent utilisé pour générer des sorties modulaires pour l'agrégation.
- Apprentissage par renforcement/rétroaction boucle : Les fonctions LLM dans un cycle interactif d'action et perception et modifie son comportement selon les commentaires reçus de un système ou un utilisateur externe.
- Utilisation autonome des outils : Le LLM est augmenté de la capacité d'invoquer outils externes (API, bases de données, systèmes de simulation, etc.) pour récupérer des informations ou effectuer des actions qui peuvent être en dehors de ses capacités principales.

Ces fonctionnalités agentiques permettent aux organisations de faire évoluer leurs opérations, d'améliorer leur efficacité et de relever des défis plus complexes en intégrant plusieurs agents ou outils spécialisés au sein d'un système cohérent. Voici deux exemples de la façon dont les architectures de référence peuvent prendre en charge différentes architectures. cas d'utilisation.

CAS D'UTILISATION 1 : SYSTÈME MULTI-AGENTS POUR LA PLANIFICATION DES OPÉRATIONS

L'IA agentique peut révolutionner la planification opérationnelle en favorisant des processus décisionnels plus dynamiques et réactifs. Par exemple, un système multi-agents pour la planification des opérations pourrait impliquer un agent commandant centralisé qui orchestre et répartit les tâches entre des agents spécialisés. Ces agents disposent de l'autonomie nécessaire pour utiliser divers outils afin de récupérer les informations requises et d'exécuter des tâches spécifiques. Le système intègre une boucle de rétroaction permettant une critique collaborative et des contrôles de conformité des plans élaborés, garantissant ainsi l'efficacité et la conformité du plan d'action final aux objectifs stratégiques.

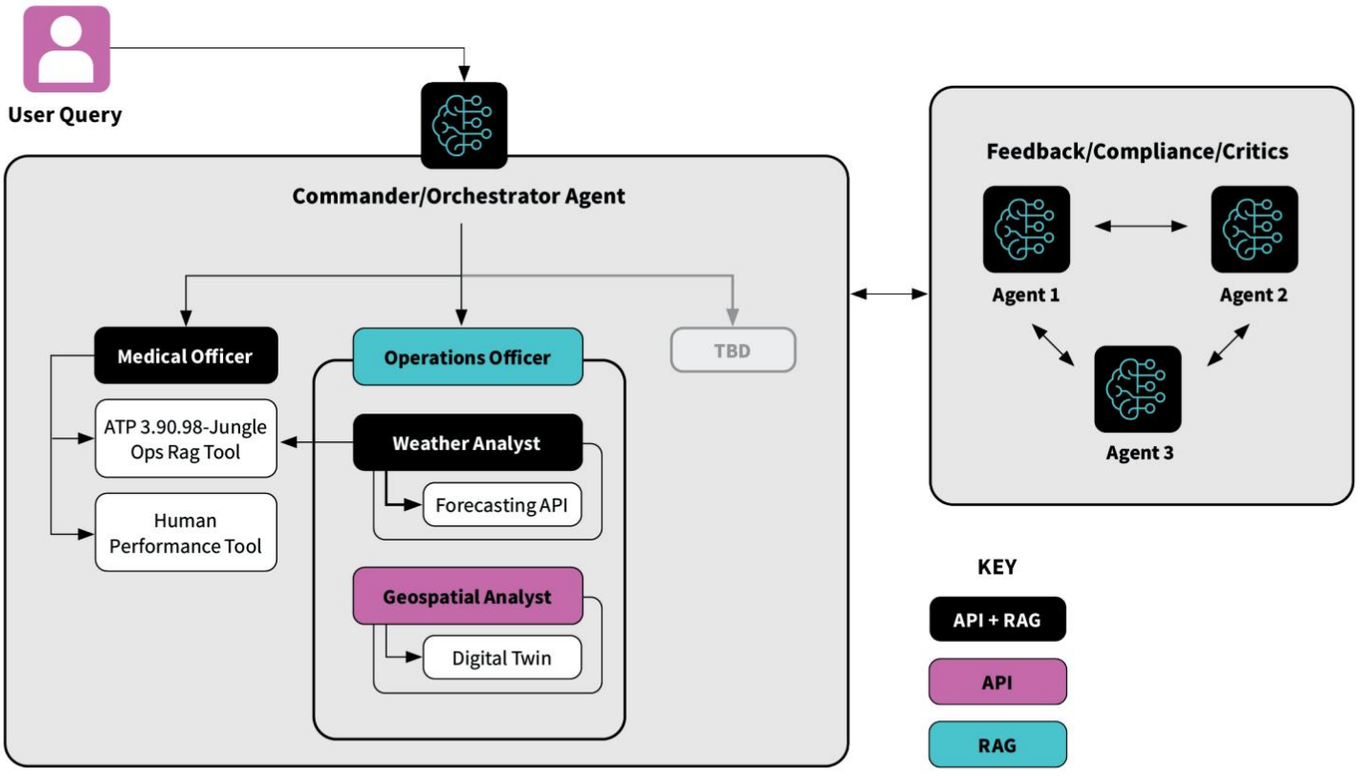


Figure 1 : Architecture de référence pour le système de planification des opérations

Machine Translated by Google

CAS D'UTILISATION 2 : SYSTÈME MULTI-AGENTS POUR LA CRÉATION DE DOCUMENTS

Dans un cas d'utilisation de création de documents, un système multi-agents implique un agent superviseur qui classe les demandes des utilisateurs selon des intentions prédéfinies et lance des workflows par étapes. Ces workflows intègrent l'interaction et la collaboration de différents agents de rédaction, chacun responsable d'aspects spécifiques de la création. Le système suit des flux logiques séquentiels qui reproduisent les comportements d'écriture humaine, garantissant ainsi la cohérence du document final et sa conformité aux exigences spécifiées.

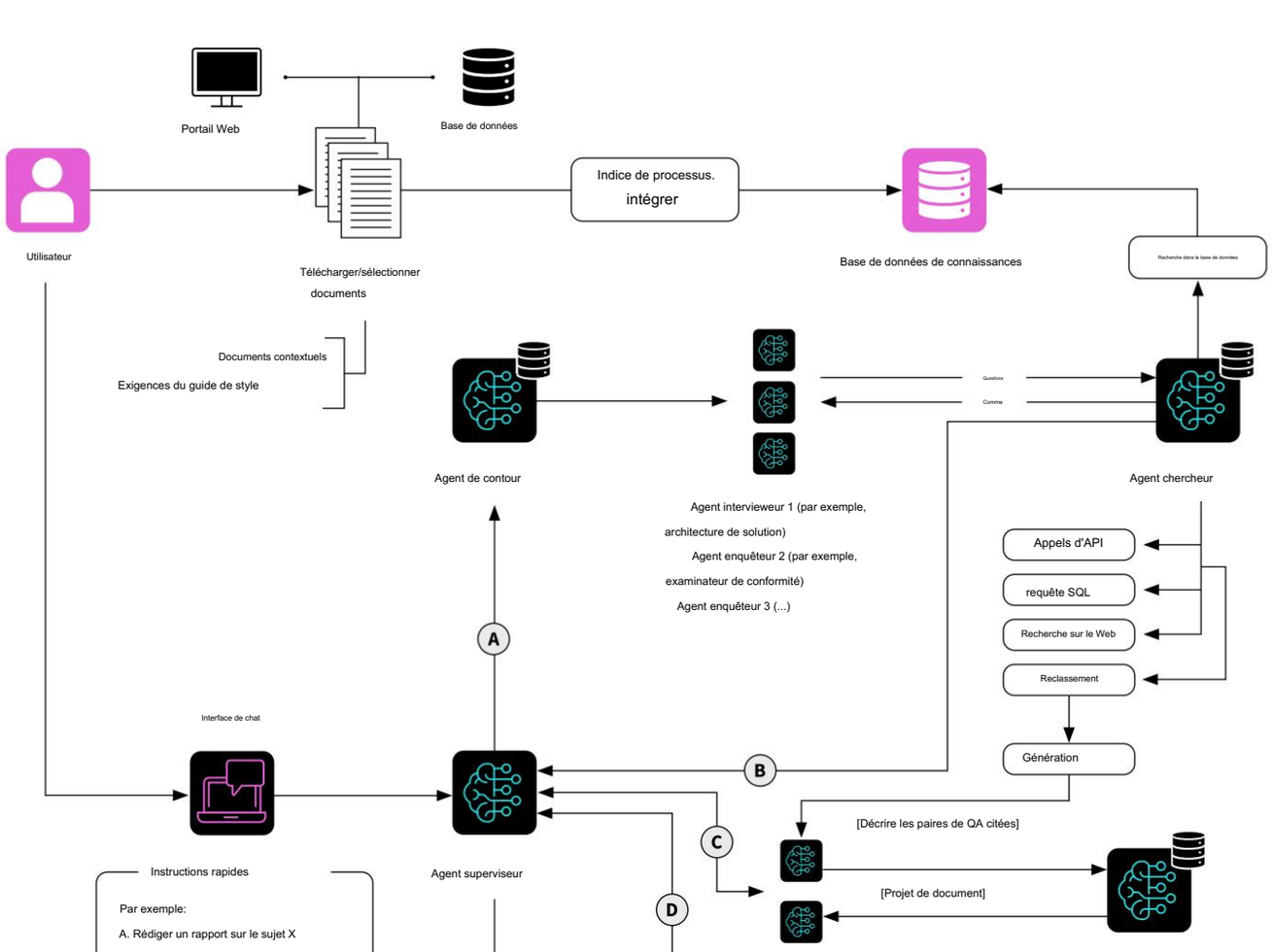


Figure 2 : Architecture de référence pour un système de co-création de documents

Ces capacités d'agent permettent aux organisations de faire évoluer leurs opérations, d'améliorer leur efficacité et de relever des défis plus sophistiqués en intégrant plusieurs agents ou outils spécialisés dans un système cohére

Machine Translated by Google

Compte tenu de l'utilité et de l'impact des systèmes orientés agents, les composants agents deviendront omniprésents dans toutes les applications et tous les systèmes logiciels à un moment donné dans un avenir prévisible.

Les systèmes agentiques offrent aux agences fédérales un potentiel de transformation en améliorant leur efficacité et en relevant des défis complexes. Par exemple, dans le cadre de la gestion des catastrophes et des urgences, un agent de commandement centralisé pourrait coordonner les agents pour récupérer des données météorologiques en temps réel, consulter des publications sur les réseaux sociaux avec photos et vidéos pour évaluer les dégâts, analyser des informations géospatiales pour les itinéraires d'évacuation et coordonner l'allocation des ressources d'urgence. Cela simplifie la prise de décision dans des délais serrés, réduit le risque d'erreur humaine et améliore la connaissance de la situation.

tous ces éléments sont essentiels dans les scénarios de haute pression.

Dans les environnements où la conformité est importante, la co-rédaction de documents par des agents peut accélérer la rédaction des politiques et garantir leur exhaustivité. En rédigeant des documents techniques, en les vérifiant pour garantir la conformité et en apportant des informations spécifiques au domaine, ces systèmes réduisent la charge de travail manuel et accélèrent le traitement des documents critiques. Bien que des risques existent, tels que la dépendance à des données incomplètes ou le comportement inattendu des agents, les utilisateurs de ces systèmes peuvent les atténuer grâce à une supervision, une collaboration réfléchie et une révision des résultats afin de garantir leur fiabilité et leur adéquation aux objectifs stratégiques.

Les « coûts de complexité » de l'IA agentique

Si l'IA agentique redéfinit les systèmes distribués en permettant des architectures hautement flexibles et auto-organisées au potentiel considérable, de nouveaux défis et compromis apparaissent. La flexibilité et l'autonomie accrues offertes par les agents engendreront simultanément une complexité exponentiellement accrue. Concevoir, gérer et garantir la fiabilité de ces systèmes nécessitera l'utilisation d'approches et de cadres sophistiqués pour maîtriser le chaos et gérer les multiples risques, décrits dans les sections suivantes.

COÛTS D'INFÉRENCE

L'IA agentique présente un potentiel considérable, mais son adoption généralisée pourrait être freinée par des coûts élevés. En effet, chaque interaction entre agents entraîne un coût lié à l'exécution des inférences. À mesure que le nombre d'agents augmente et que leur autonomie s'accroît, les dépenses de calcul augmentent proportionnellement. Or, nous ne disposons aujourd'hui d'aucune certitude, ni même d'estimations fiables, quant au coût et à l'ampleur de cette interaction dynamique. Des chercheurs de l'Université de Princeton ont constaté que les recherches actuelles sur les agents d'IA se concentrent souvent étroitement sur la précision, négligeant l'analyse des mesures de contrôle des coûts. Cependant, le coût du matériel et des calculs tend à diminuer avec le temps. Bien qu'il puisse être très élevé aujourd'hui, il pourrait devenir raisonnable pour la plupart des entreprises d'ici deux ans.

PROBLÈMES DE MISE À L'ÉCHELLE

Le comportement gourmand en ressources des agents, qui réfléchissent ou négocient constamment des tâches, crée d'importants défis opérationnels. Contrairement aux microservices traditionnels qui exécutent des tâches prédéfinies de manière efficace et prévisible, les agents autonomes peuvent traiter des données en temps réel, prendre des décisions et s'adapter en continu aux conditions changeantes. Plus le nombre d'agents dans un système augmente, plus leurs interactions sont complexes. Les solutions évolutives doivent gérer efficacement cette charge accrue sans compromettre les performances.

LACUNES EN MATIÈRE DE FORMATION ET DE DONNÉES

Former les agents avec des données pertinentes présente un autre défi. Les agents autonomes sont plus efficaces lorsqu'ils sont entraînés à certaines tâches, actions ou raisonnements. Entraîner ces agents à un domaine spécialisé ou à une nouvelle tâche nécessite souvent d'énormes quantités de données de haute qualité. Par exemple, pour des tâches telles que la transcription, la synthèse et l'analyse des sentiments, de vastes ensembles de données doivent représenter la diversité du monde réel. et nuances. Ces tâches nécessitent une compréhension du contexte, du ton et des subtilités linguistiques, qui varient selon les domaines. Une formation approfondie pour gérer ces variations est la clé de la réussite des déploiements.

SÉCURITÉ ET STABILITÉ

Le couplage faible des systèmes d'IA agentique présente des risques importants pour la sécurité et la stabilité. Les agents autonomes évoluent et adaptent leur comportement au fil du temps. Cette flexibilité, bien qu'offrant des avantages évidents, peut entraîner des évolutions inattendues, exposant des vulnérabilités ou se comportant de manière imprévisible. Des inquiétudes naissent également du risque que des agents communiquent dans des formats que les humains ne peuvent ni lire ni comprendre. En optimisant leurs interactions, les agents peuvent développer des protocoles de communication véritablement opaques, allant au-delà du langage naturel, ce qui complique considérablement le processus d'audit et de compréhension de leurs décisions et actions. Si les agents décident que la communication binaire est plus efficace, comment les humains pourront-ils un jour reprendre le dialogue ? Pour garantir la confiance et la sécurité de ces systèmes, de nouveaux outils permettant d'enregistrer, de surveiller et d'auditer les interactions des agents apparaîtront probablement.

ÉTHIQUE ET CONFIDENTIALITÉ

À mesure que les agents autonomes assument davantage de responsabilités, déterminer qui ou quoi est responsable de leurs actions devient complexe. Les cadres de responsabilisation traditionnels, qui reposent sur la supervision humaine, peuvent s'avérer insuffisants. Si les organisations ne traitent pas les données de manière responsable et conforme aux réglementations en matière de confidentialité et de sécurité, la confiance des parties prenantes risque d'être perdue. Les processus décisionnels des agents sont-ils exempts d'erreurs et de biais ? Il peut être difficile, voire impossible, de le savoir.

certains cas.

Machine Translated by Google

L'avenir des agents : l'équilibre Autonomie, fonctionnalité et contrôle

L'évolution rapide des systèmes à base d'agents bouleversera probablement les architectures logicielles traditionnelles, les agents d'IA devenant de plus en plus capables d'effectuer un large éventail de tâches. Avec l'intégration croissante d'agents dans les applications, des modèles d'architecture multi-agents courants émergeront, cristallisant le besoin de :

- Documenter et tester l'applicabilité de chaque modèle d'architecture et les cas d'utilisation qu'il permet
- Établir des fonctions d'entreprise pour l'orchestration, la surveillance, la gestion, la sécurité des agents, etc.
- Établir méthodiquement les meilleures pratiques qui calibrent le cas d'utilisation, la valeur, le coût de calcul et la complexité de l'architecture

L'adoption d'architectures orientées agents pourrait signifier un abandon des architectures orientées services et basées sur des API. Si les intégrations d'API resteront nécessaires pour certains types de transactions et de fonctions (par exemple, déterministes et récurrentes), les architectures orientées agents pourraient se prêter à l'exécution de fonctions et de tâches non déterministes, notamment celles qui n'ont jamais été abordées auparavant. Un jour, une équipe d'agents pourrait même décider collectivement quel algorithme GenAI utiliser pour son prochain projet, un peu comme choisir le meilleur « cerveau » pour la tâche.

Étant donné l'utilité et l'impact des systèmes orientés agents, les composants agents deviendront omniprésents dans toutes les applications et tous les systèmes logiciels à un moment donné dans un avenir prévisible. Il est probable que les logiciels commerciaux adopteront une approche axée sur les agents et fourniront l'accès non seulement aux API, mais aussi aux agents pour des interactions et des fonctions complexes. Exploiter ces nouvelles capacités pour résoudre les problèmes des clients et assurer l'adéquation produit-marché sera crucial pour les entreprises technologiques.

De nombreux défis restent à relever concernant les protocoles de communication interagents, les mécanismes de découverte et d'enregistrement des agents, l'amélioration des compétences en fonction des retours d'expérience de l'environnement, etc. Par exemple, les solutions d'agents actuelles sont principalement conçues pour les interactions humaines, comme l'IA conversationnelle en langage naturel, plutôt que pour les communications orientées machine, typiques des appels d'API web.

Pour rendre les systèmes d'IA agentiques opérationnels de manière sûre et productive, les organisations se concentreront probablement sur des stratégies de base d'atténuation des risques, avec des tests et une validation approfondis des systèmes d'IA agentiques avant leur déploiement, ainsi que la création de protocoles de surveillance et d'intervention humaines si nécessaire. De nouvelles recherches sur la gouvernance des données et les normes éthiques liées à l'autonomie contribueront à prévenir les abus d'agents ou les manquements éthiques susceptibles de nuire à la réputation et aux finances. Des systèmes de contrôle efficaces seront nécessaires de toute urgence pour surveiller et réguler le comportement des agents, les empêchant de dévier de leurs fonctions initiales ou de se livrer à des activités préjudiciables. Des recherches sur les plateformes d'audit, la traçabilité et les techniques seront nécessaires pour consigner chaque interaction des agents entre eux.

Il est également important de considérer que la nature décentralisée des systèmes d'IA agentique peut être particulièrement difficile à concilier, du moins dans un premier temps, avec l'exigence d'une responsabilité stricte au sein du secteur fédéral. Garantir que les agents autonomes opèrent dans des limites éthiques et juridiques définies nécessite d'emblée la mise en place de cadres de gouvernance robustes. L'évolutivité de ces systèmes doit également être soigneusement gérée pour gérer les vastes volumes de données et les interactions complexes caractéristiques des opérations fédérales.

Il n'existe pas encore de systèmes de production impliquant des centaines d'agents travaillant simultanément, mais l'IA agentique représente une avancée révolutionnaire en matière d'innovation. Son évolution est si rapide que les organisations devraient commencer à expérimenter ces outils dès maintenant, dans un environnement sandbox, afin de tester leur capacité à comprendre et à piloter efficacement les agents. En mettant en œuvre des stratégies de prototypage, de test et d'atténuation des risques adaptées, les organisations se positionneront pour exploiter les nombreux avantages techniques de l'IA agentique tout en garantissant un fonctionnement éthique, innovant, transformateur et sûr de ces systèmes.

John Larson dirige la pratique de l'IA de Booz Allen en veillant à ce que les dirigeants des missions fédérales parviennent à une compréhension de l'IA, à des solutions spécialement conçues et à une adoption accélérée.

Alison Smith, directrice de l'IA générative chez Booz Allen, dirige les solutions GenAI dans toute l'entreprise et aide les équipes à créer les meilleures pratiques pour le développement et l'utilisation de l'IA.

LECTURE RAPIDE

L'IA agentique est la prochaine évolution de l'IA générative et conduira à des systèmes informatiques distribués et multi-agents capables de s'adapter et même de résoudre des problèmes sans intervention humaine.

L'IA agentique bouleversera les architectures logicielles traditionnelles. Elle pourrait même nécessiter l'abandon des architectures orientées services et basées sur des API, car des agents hautement spécialisés, basés sur de vastes modèles de langage, seront de plus en plus capables d'exécuter un large éventail de tâches, seuls ou en collaboration.

Les cas d'utilisation potentiels de l'IA agentique incluent la planification des opérations et la création de documents, mais les défis et les coûts de cette technologie, qui incluent des problèmes d'évolutivité, des besoins de formation des données et des problèmes de sécurité, nécessitera le développement de cadres et d'outils pour gérer efficacement ces systèmes complexes.

Où algorithmes Rencontrer Compte

stabilité

Protection des données dans la lutte croissante pour la confidentialité

Max Wragan, Edward Raff et Sean Guillory

Confidentialité a longtemps été considéré comme un droit fondamental dans les sociétés démocratiques, mais La confidentialité des données risque de devenir une illusion. Les nouvelles technologies et la prolifération des données rendent difficile la protection de la confidentialité des informations personnelles. En octobre 2024, Forbes Des chercheurs ont rapporté que deux étudiants de Harvard avaient utilisé des lunettes connectées, l'IA et des données en ligne pour identifier des personnes qu'ils n'avaient jamais rencontrées et localiser leurs informations personnelles. Les auteurs d'une étude publiée dans la revue Patterns On estime qu'il était possible d'identifier de manière unique 93 % des personnes dans un ensemble de données de 60 millions de personnes en utilisant seulement quatre éléments de données auxiliaires.

Machine Translated by Google

La protection de la vie privée, qui inclut le maintien de la confidentialité des données, est une question de confiance publique. Lorsque les citoyens ne font pas confiance aux entreprises et aux institutions pour respecter leur vie privée et agir de manière responsable, leur confiance en elles s'érode. Le Pew Research Center rapporte qu'environ 7 adultes américains sur 10 s'inquiètent de la manière dont le gouvernement utilise les données qu'il collecte à leur sujet. Selon cette même étude, 81 % des Américains déclarent que les informations collectées par les entreprises seront utilisées à des fins qui les gênent.

Ces gros titres et reportages négatifs, qui détaillent les menaces croissantes pesant sur la confidentialité des données, occultent une vérité fondamentale : la collecte et l'analyse de données ne sont pas intrinsèquement mauvaises. Au contraire, le partage de données de manière sûre et responsable présente un intérêt considérable. Lorsque les hôpitaux partagent des données de manière confidentielle et mutuellement convenue, par exemple, les médecins peuvent mener davantage de recherches avec des partenaires externes, ce qui accélère l'innovation médicale et conduit à des traitements potentiellement vitaux. Lorsque les agences fédérales chargées de la sécurité publique et nationale peuvent combiner des ensembles de données sensibles, elles peuvent identifier les menaces plus tôt et mieux protéger les citoyens.

La mise en place de mesures de protection des données appropriées accélérera l'innovation. C'est particulièrement vrai dans le domaine de l'IA, où les modèles doivent accéder à de vastes volumes de données utiles et propres pour acquérir de nouvelles fonctionnalités et optimiser leurs performances. Trouver un équilibre entre le problème croissant de la confidentialité des données et les avantages d'un partage sûr et responsable des données exige une compréhension plus approfondie du paysage de la confidentialité. Sur cette question, le gouvernement fédéral a l'occasion de montrer la voie en adoptant de nouvelles techniques et en soulignant constamment l'importance de la confidentialité des données. Dans cet article, nous décrivons les défis liés à la confidentialité des données et examinons plusieurs techniques pour les atténuer.

Des données, des données partout

La cause profonde du problème de confidentialité des données réside dans le volume considérable de données en circulation. Les organisations de tous secteurs collectent des données à un niveau sans précédent. Selon l'entreprise Skynova, « 64 % des chefs d'entreprise et dirigeants » collectent des données clients sur les réseaux sociaux.

Les organismes de santé collectent des données pour améliorer les soins aux patients et suivre les tendances en matière de santé. Même le gouvernement fédéral collecte des données, comme indiqué dans la Responsabilité gouvernementale. Site Web du bureau, « Le gouvernement fédéral recueille et utilise des renseignements personnels sur les individus de manière de plus en plus sophistiquée, notamment pour l'application de la loi, le contrôle des frontières et l'amélioration des interactions en ligne avec les citoyens. »

Le problème est que les techniques couramment utilisées pour protéger les données collectées et préserver leur confidentialité – la norme de k-anonymat, les statistiques récapitulatives, l'agrégation d'informations et leurs modèles prédictifs basés sur une interface de programmation d'application (API) – ne sont pas toujours suffisantes. Il existe également la menace de cybercriminels qui s'introduisent dans un système et volent des données. En d'autres termes, la promesse contenue dans les politiques de confidentialité classiques – « nous ne partagerons jamais vos informations personnelles » – omet une mise en garde importante : intentionnellement.

Le problème est encore aggravé par la disponibilité d'algorithmes et de modèles d'IA puissants, qui permettent aux acteurs malveillants d'exploiter plus facilement des ensembles de données incomplets ou partiellement expurgés pour les recouper et les désanonymiser, leur permettant ainsi d'extraire des informations jusque-là considérées comme protégées. À mesure que de plus en plus d'informations personnelles circulent en ligne, intentionnellement ou non, les acteurs malveillants disposeront de plus de données à exploiter, ce qui compliquera considérablement les efforts futurs de protection de la confidentialité des données.

Une approche différente d'un Problème croissant

Apple, Google, Microsoft et des instances bien informées du gouvernement américain utilisent un ensemble de techniques communément appelées « privilège différentiel » pour garantir la confidentialité des données. Ce cadre mathématique introduit du « bruit », ou variation aléatoire, dans un ensemble de données afin de masquer des points de données individuels. À l'instar d'un filtre photo floutant les traits du visage, le privilège différentiel limite les informations visibles et extrayables une fois les données partagées, que ce soit via un appel d'API, une base de données ou un algorithme de machine learning.

La confidentialité différentielle n'est pas parfaite. Elle exige des utilisateurs qu'ils réfléchissent et prennent en compte les informations qu'ils divulguent chaque fois qu'ils donnent accès à leurs données. Il est également impératif d'ajouter du bruit judicieusement. Lorsque le niveau optimal de bruit est ajouté, les informations agrégées pouvant être extraites (comme les moyennes, les intervalles et les vraisemblances statistiques) ne sont pas significativement modifiées par l'injection de différences aléatoires dans les enregistrements individuels. En revanche, un bruit excessif nuit à la précision des données.

L'avantage de la confidentialité différentielle est ce qu'elle garantit : lorsqu'un ensemble de données est partagé sous son voile, le destinataire ne peut rien faire pour en extraire plus de données que ce que le propriétaire souhaite révéler.

Mettre les données appropriées les mesures de protection de la vie privée en place accélérer l'innovation. C'est particulièrement vrai dans le domaine de L'IA là où les modèles ont besoin d'accès à de larges étendues de terres utiles et propres données pour apprendre de nouvelles capacités et optimiser leurs performances.

Figure 1 : Dissiper les idées fausses sur la confidentialité des données

IDÉE FAUSSE	RÉALITÉ
Les organisations peuvent contrôler et auditer entièrement l'utilisation des données de l'IA.	Les systèmes d'analyse et d'IA peuvent créer des résultats difficiles à tracer, ce qui fait de l'audit de l'utilisation des données un défi majeur pour toute organisation.
L'anonymisation des données empêche le traçage des données sensibles.	Les données anonymisées peuvent souvent être réidentifiées en reliant des ensembles de données.
Les contrôles d'accès empêchent l'accès non autorisé aux données.	Bien que les contrôles d'accès soient un bon outil pour prévenir les accès non autorisés, des attaquants sophistiqués peuvent toujours exploiter les vulnérabilités du système pour accéder à des données sensibles.
Les politiques de conservation des données imposent la suppression des données selon des calendriers établis.	Les systèmes hérités et les données décentralisées peuvent entraîner une conservation des données au-delà des mandats politiques.
Le respect des réglementations en matière de confidentialité garantit des risques d'exposition atténués.	Les cadres réglementaires sont souvent en retard sur les avancées technologiques, exposant ainsi les systèmes à des risques pour la vie privée.

Confidentialité différentielle en action

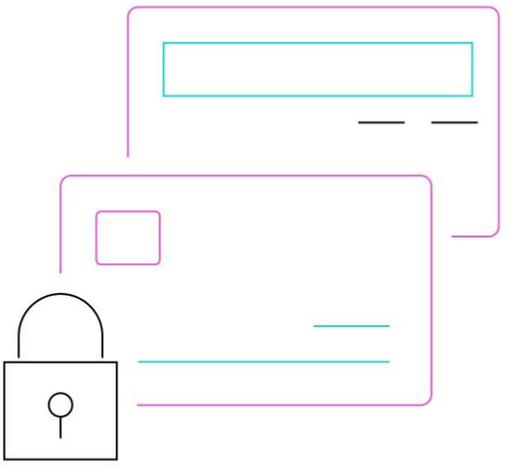
Le recensement américain de 2020 a été l'un des plus importants déploiements de confidentialité différentielle à ce jour, et l'un des cas d'utilisation les plus risqués en matière de protection des données, car les données collectées lors du recensement déterminent la représentation politique et la répartition des fonds publics. Dans une étude publiée dans Science, Les chercheurs ont vérifié que les méthodes utilisées protégeaient efficacement la confidentialité des répondants. Ils ont également constaté que si la confidentialité différentielle préservait l'exactitude des données aux niveaux étatique, régional et national, elle était compromise à l'échelle du quartier, ce qui pouvait entraîner une sous-représentation ou une surreprésentation de certains groupes, notamment les minorités raciales et ethniques.

Ce résultat illustre un point important : en général, plus l'ensemble de données est volumineux, plus il est facile de garantir la confidentialité sans compromettre l'utilité des données. Cependant, le compromis dépend fortement des objectifs de l'analyse. Si l'on souhaite simplement calculer l'âge moyen d'une population entière, la confidentialité différentielle est réalisable avec seulement 100 enregistrements. Si l'on souhaite déterminer l'âge moyen d'un groupe spécifique selon plusieurs critères démographiques supplémentaires, il faudrait ajouter du bruit pour protéger les enregistrements individuels. De même, la confidentialité différentielle est plus difficile à obtenir en présence de valeurs aberrantes significatives. Dans les données relatives à l'impôt sur le revenu, par exemple, la plupart des méthodes de confidentialité peinent à masquer les milliardaires, car leurs données se distinguent fortement de celles des autres.

Machine Translated by Google

Réaliser l'investissement

La protection de la vie privée a un coût. Nombre des meilleures techniques, notamment la confidentialité différentielle, commencent tout juste à se répandre dans l'industrie et se situent actuellement au sommet de la courbe des coûts. Pour les problèmes nécessitant une solution sur mesure, une agence fédérale peut devoir dépenser entre 1 et 10 millions de dollars pour la recherche, le pilotage et le développement de son propre programme de confidentialité différentielle.



Ces coûts ne sont pas insurmontables et s'inscrivent largement dans les budgets de nombreuses agences fédérales. Ils sont également dérisoires comparés aux sanctions financières que les organisations encourent lorsqu'elles ne protègent pas correctement les données personnelles. Un juge fédéral a ordonné à l'Office of Personnel Management de verser 63 millions de dollars à des fonctionnaires fédéraux, anciens et actuels, ainsi qu'à des candidats à un emploi, touchés par une violation de données.

Figure 2 : Les points forts et les points faibles de trois techniques de protection des données

Technique de protection des données	Limitations et cas d'utilisation optimaux
Les données synthétiques permettent de créer des ensembles de données artificiels dont les propriétés statistiques sont similaires à celles des ensembles de données réels. Leurs propriétés statistiques miroir permettent aux utilisateurs d'obtenir des informations précieuses grâce à l'entraînement des modèles et à l'analyse des données, sans compromettre les informations sensibles contenues dans les ensembles de données réels auxquels elles sont censées ressembler. Cependant, les performances et la ressemblance des données synthétiques sont réduites lors de tâches plus détaillées, avec des sous-échantillons de données plus petits.	Les ensembles de données synthétiques sont moins complexes que les ensembles de données réels, ce qui nécessite une gestion rigoureuse des données et des stratégies supplémentaires d'atténuation des biais pour les analyses susceptibles d'avoir un impact sur certaines sous-sections de données, comme les groupes minoritaires sous-représentés. L'utilisation de données synthétiques est particulièrement adaptée aux situations où la précision du modèle peut être moins importante que la protection de la confidentialité, comme la recherche en santé ou la détection des fraudes.
L'apprentissage fédéré réduit les risques liés à l'exposition des données en permettant aux modèles d'apprentissage automatique de s'entraîner sur des appareils décentralisés qui protègent les données en les conservant localement. Il amène le modèle aux données, plutôt que les données au modèle. Les modèles apprennent localement sur les appareils, et les mises à jour et améliorations qu'ils obtiennent grâce à cet entraînement sont renvoyées à un serveur central.	Au sein du secteur de la santé, l'apprentissage fédéré a été déployé pour protéger la confidentialité des données des patients et pour améliorer l'utilité des modèles cliniques pour les patients, comme la plateforme de segmentation tumorale fédérée (FeTS) de l'Université de Pennsylvanie. Cependant, la technique n'est pas adaptée à tous les cas d'utilisation, car une distribution inégale des données ou des types de données entraîne des obstacles fréquents et une latence pour les applications d'apprentissage fédéré.
Le chiffrement homomorphe permet aux analystes d'effectuer des calculs sur les données sans les déchiffrer au préalable. Cette technique est particulièrement avantageuse lorsque la confidentialité est primordiale (par exemple, dans le cadre de transactions financières). Préserver le chiffrement pendant le calcul présente également des avantages pratiques : il permet aux analystes externes ou tiers de traiter les données sans accéder aux informations brutes.	Bien que cette technique soit bien adaptée aux ensembles de données très sensibles mais de petite taille, des limites pratiques sont présentes avec des ensembles de données plus volumineux en raison de la nature intensive en calcul qui entraîne des retards et des dépenses importants lors d'une utilisation à grande échelle.

Machine Translated by Google

De plus, la protection de la vie privée des citoyens est une responsabilité essentielle des gouvernements démocratiques. Grâce à une collaboration continue entre le gouvernement, l'industrie et les universités,
Des solutions plus abordables seront disponibles. Par exemple,
Les modèles de classification de texte étaient autrefois presque impossibles à
Entraînez-vous de manière différentiellement privée avant que le bruit ne détruise la rareté des ensembles de données, ce qui a considérablement augmenté le temps et le coût de formation des modèles.

En réfléchissant soigneusement aux objectifs et en tenant compte des sources de bruit nécessaires, il est désormais possible de réduire le temps de formation de plusieurs mois à quelques minutes. Pour y parvenir, il faut comptabiliser soigneusement et délibérément les informations contenues dans l'algorithme et leur destination, mais le résultat est significatif.
L'investissement initial vaut largement le retour sur investissement à long terme : une fois que ces optimisations deviennent reproductibles, le coût des déploiements ultérieurs diminue.

Lorsqu'il s'agit de plaider en faveur d'investissements accrus dans la confidentialité des données, le coût en dollars n'est peut-être pas le plus gros obstacle.
Bien plus redoutable est la combinaison de cultures organisationnelles réticentes au partage d'informations, combinée à un manque de compréhension des nouvelles solutions de confidentialité des données.
Lorsque les dirigeants ne comprennent pas pleinement les défis à relever ou les solutions disponibles, ils sont moins susceptibles de défendre un programme qui nécessite des investissements et un changement culturel.

Mais un manque de compréhension ne constitue pas une raison valable pour retarder la mise en œuvre de solutions de confidentialité des données. Les agences fédérales ont l'obligation de faire progresser les technologies de confidentialité des données dans le cadre d'une IA responsable, une réalité reconnue au plus haut niveau. Selon le décret exécutif de 2023 sur
le développement et l'utilisation sûrs, sécurisés et dignes de confiance de l'intelligence artificielle : « Le gouvernement fédéral appliquera les lois et les principes existants en matière de protection des consommateurs et adoptera des mesures de protection appropriées contre la fraude, les préjugés involontaires, la discrimination, les atteintes à la vie privée et autres préjudices causés par l'IA. »

Le décret exécutif 14110 demande ensuite à l'Institut national des sciences et de la technologie (NIST) de créer des lignes directrices pour
Les agences doivent évaluer l'efficacité des protections différentielles de confidentialité, y compris celles de l'IA. Au moment de la mise sous presse de cet article, le NIST indiquait qu'un rapport final serait publié.
était en cours.

Voies alternatives vers la confidentialité et techniques complémentaires

La confidentialité différentielle offre un avantage unique en traitant le risque de confidentialité de manière incrémentale, contrairement à de nombreuses autres techniques qui simplifient souvent excessivement la confidentialité en la qualifiant de « protégée » ou de « non protégée ». Bien que ces méthodes alternatives puissent fournir une couche de confidentialité et de sécurité des données, elles ne sont pas infaillibles. Avec les volumes croissants de données collectées et souvent insuffisamment protégées, le risque d'exposition augmente à chaque traitement. C'est là que la confidentialité différentielle se distingue : elle garantit que le risque de réidentification reste dans les limites définies par son cadre mathématique, quelle que soit la quantité de données sur un individu déjà disponible.

Toutefois, dans les cas où la confidentialité différentielle s'avère trop difficile à mettre en œuvre ou incompatible avec la situation, des techniques alternatives peuvent contribuer à atténuer le risque d'exposition. Parmi ces techniques figurent les données synthétiques, l'apprentissage fédéré et le chiffrement homomorphe. Elles peuvent renforcer la protection des données lorsque la confidentialité différentielle est impossible ou renforcer les solutions de confidentialité différentielle lorsqu'elles sont en place.

Max Wragan dirige la stratégie d'IA et la gestion des risques pour aider Booz Allen et ses clients à déployer l'IA et les outils d'IA pour améliorer de manière responsable la réalisation de projets avec une technologie de pointe.

Edward Raff, Ph.D., dirige l'équipe de recherche en apprentissage automatique (ML) de Booz Allen, développe des talents techniques de haut niveau et diffuse les dernières compétences, techniques et connaissances en ML dans toute l'entreprise.

Sean Guillory, Ph.D., est un scientifique principal sur les projets d'opérations du domaine cognitif et un responsable de programme d'IA pour l'AI Rapid Prototyping Museum.

LECTURE RAPIDE

Les algorithmes avancés et les outils d'IA facilitent la violation de la confidentialité des données, les incidents récents montrant avec quelle facilité des informations personnelles peuvent être extraites d'ensembles de données apparemment protégés.

La confidentialité différentielle, un cadre mathématique qui introduit un bruit contrôlé dans les ensembles de données, offre une solution prometteuse, comme le démontre son utilisation réussie dans le recensement américain de 2020.

Bien que la mise en œuvre de solutions de confidentialité robustes nécessite des investissements importants, les agences fédérales ont à la fois la responsabilité et la possibilité de mener l'innovation en matière de protection de la confidentialité des données.

Depuis les lignes de front de Cryptographie post-quantique

PROTECTION DES INFRASTRUCTURES CRITIQUES CONTRE ÉVOLUTION DES CYBERMENACES

Taylor Brady, Jordan Kenyon et Derek Aucoin

La cryptographie quantique (PQC) sera l'un des défis majeurs en matière de cybersécurité de la prochaine décennie . Les normes PQC tant attendues du National Institute of Standards and Technology (NIST) sont enfin disponibles. Elles définissent les exigences et les spécifications de mise en œuvre des algorithmes quantiques approuvés. Cependant, la mise en œuvre de la PQC sera un processus complexe. L'Office of Management and Budget (OMB) estime qu'entre aujourd'hui et 2035, les transitions vers la PQC coûteront plus de 7 milliards de dollars aux agences fédérales. Cette estimation exclut explicitement les systèmes de sécurité nationale et ne tient pas compte des coûts d'adoption du PQC dans le secteur commercial. Il est difficile de sous-estimer l'ampleur de cette transition.

Les ordinateurs quantiques finiront par démanteler la quasi-totalité des systèmes de cryptographie à clé publique actuellement déployés – les algorithmes profondément ancrés dans le matériel, les logiciels et les protocoles numériques qui protègent les réseaux des acteurs malveillants. La question est de savoir quand et non si. D'importants défis techniques doivent encore être relevés avant que les ordinateurs quantiques atteignent l'échelle et la robustesse nécessaires à l'exécution d'algorithmes menaçant la cryptographie à clé publique. Malgré ces obstacles, de nombreuses feuilles de route commerciales prévoient que de tels dispositifs pourraient être disponibles vers 2030.

Ce calendrier accéléré accroît la pression sur les organisations pour qu'elles adoptent au plus vite les nouvelles normes PQC du NIST. L'urgence est encore plus grande pour les organisations disposant d'ensembles de données sensibles dont la durée de conservation est plus longue.

Transition vers le post-quantique

Durée de conservation des données. Ces données pourraient déjà être la cible d'attaques « Hold Now, Decrypt Later » (HNDL), par lesquelles un État-nation ou une organisation criminelle s'infiltre dans un réseau, vole des données chiffrées et les stocke sur ses propres serveurs, sachant qu'il pourra y accéder dès que des ordinateurs quantiques capables de percer la cryptographie à clé publique seront disponibles. Le Centre d'études stratégiques et internationales a mis en évidence la menace réelle que représentent les attaques HNDL, soulignant ainsi l'importance pour les agences fédérales de migrer sans tarder vers la PQC.

Bien qu'un nombre croissant d'exigences fédérales commencent à structurer la manière dont les agences abordent la PQC, la feuille de route pour y parvenir n'est pas aussi linéaire qu'il y paraît. Les responsables de la sécurité de l'information (RSSI) fédéraux disposent d'une grande latitude pour concevoir des stratégies de PQC adaptées à la surface d'attaque et aux vecteurs de menace spécifiques de leur agence. Les entreprises commerciales disposent d'une latitude encore plus grande. En pratique, cela signifie que le point de départ de la démarche PQC des organisations importe moins que la manière dont elles accomplissent chaque phase.

Heureusement, les expériences des premiers utilisateurs offrent des enseignements clés aux entreprises qui se lancent dans les trois étapes principales de la préparation au PQC : la découverte cryptographique, le prototypage et l'agilité.

LES BASES

1. Les ordinateurs quantiques finira par briser presque toute la cryptographie à clé publique actuellement déployée.

   C'est pourquoi il est impératif que les agences gouvernementales et les entreprises privées commencent à prendre des mesures pour protéger leurs actifs avec de nouveaux algorithmes cryptographiques.

2. La cryptographie post-quantique (PQC) fait référence à la mise en œuvre d'algorithmes capables de résister à une attaque cryptanalytique par un ordinateur quantique.

   Il s'agit de la meilleure défense actuellement disponible pour contrer la cybermenace posée par les ordinateurs quantiques à grande échelle. Cependant, la mise en œuvre du PQC ne sera pas simple et les organisations doivent agir sans délai.

3. La transition vers le PQC est particulièrement urgente pour certaines organisations fédérales et commerciales étant donné le risque d'attaques HNDL.

   Avec une attaque HNDL, un adversaire acquiert des informations qui n'ont pas encore été resécurisées avec PQC et stocke ces actifs jusqu'à ce qu'un ordinateur quantique capable de briser ce cryptage soit disponible.

Machine Translated by Google

Découverte cryptographique : cartographie de la surface d'attaque

La découverte cryptographique consiste à créer un inventaire cryptographique exploitable et hiérarchisé, en détectant, traçant et évaluant la cryptographie utilisée dans une entreprise en fonction de sa sécurité à l'ère post-quantique. La découverte cryptographique est un objectif intuitif, mais il peut s'avérer extrêmement difficile à atteindre. Les outils de cybersécurité courants détectent la cryptographie par conception, mais ne cataloguent pas les cryptographies vulnérables pour permettre leur priorisation et leur correction. De ce fait, la plupart des outils sont mal équipés pour offrir aux organisations la visibilité nécessaire sur les vulnérabilités cryptographiques générées par les nouvelles technologies d'informatique quantique.

De nombreux nouveaux produits apparaissent sur le marché pour combler cette lacune, mais l'ajout d'outils de sécurité supplémentaires a un coût : il augmente à la fois le coût total et le temps de migration. Ce temps est souvent négligé par les organisations, compte tenu des risques d'attaques de type « Conserver maintenant, déchiffrer plus tard » et des ressources inutiles. Plutôt que d'acquérir de nouveaux produits, certaines organisations se tournent vers de nouvelles méthodes d'ingénierie des données pour surmonter les défis courants liés à la découverte cryptographique.

ÉTUDE DE CAS

Lorsque le gouvernement américain a tiré la sonnette d'alarme sur la criticité du PQC en 2022 par le biais de la sécurité nationale Une entreprise de vente au détail du Fortune 10 a pris note du Mémorandum 10, la loi sur la préparation à la cybersécurité de l'informatique quantique , et du Mémorandum de l'OMB sur la migration vers la cybersécurité de l'informatique quantique. Elle a constaté qu'investir dans une plateforme d'analyse évolutive et de niveau production pour découvrir dynamiquement la cryptographie sur ses vastes systèmes fédérés lui permettait de comprendre son exposition aux risques sans avoir recours à de nouvelles mesures de cybersécurité.

Des pipelines d'extraction, de transformation et de chargement (ETL) ont été utilisés pour optimiser l'utilisation des métadonnées cryptographiques des capteurs existants et assurer la traçabilité des certificats et des connexions uniques. Ainsi, les responsables de la sécurité de l'organisation pouvaient utiliser le tableau de bord pour visualiser en temps réel la puissance cryptographique du réseau, et les analystes pouvaient remonter à la source des vulnérabilités cryptographiques pour les corriger, soumettre des requêtes personnalisées et étendre la couverture de l'outil de découverte à de nouvelles frontières réseau.

POINTS CLÉS À RETENIR

1. COMMENCEZ PETIT

   Définissez un réseau prioritaire pour une initiative initiale de découverte cryptographique, en reconnaissant que tout ne peut pas être transféré en même temps.

2. OPTIMISER LA RÉUTILISATION

   Extrayez les données cryptographiques des capteurs existants sur le réseau pour augmenter la vitesse de résolution et éviter les coûts d'infrastructure et la complexité supplémentaires.

3. CONCEVOIR LA FLEXIBILITÉ Investissez

   dans une plateforme évolutive qui peut être utilisée à la fois pour les inventaires initiaux lors de la planification du PQC et pour la surveillance continue pendant la mise en œuvre du PQC.

Machine Translated by Google

Prototypage : mettre le PQC à l'épreuve

La découverte cryptographique est un point de départ courant dans le parcours vers la sécurité post-quantique, mais ce n'est pas le seul endroit où une entreprise peut faire ses premiers pas vers la PQC.
La découverte permet aux organisations d'élargir leur planification PQC ; le prototypage permet d'approfondir. Le prototypage se concentre sur la modélisation et la mesure des impacts de la transition vers le PQC sur les performances et l'interopérabilité.

Les principes mathématiques de la PQC sont fondamentalement différents de ceux de la cryptographie à clé publique traditionnelle. Sa complexité de calcul accrue fait de la PQC une défense robuste contre les attaques quantiques. Elle pose également des défis en matière de réseau et d'infrastructure, tels qu'une latence et une bande passante accrues, et un manque d'interopérabilité. Comprendre l'impact de ces défis est essentiel pour éclairer les décisions d'achat, de mise en œuvre et le choix des algorithmes dans les cas d'utilisation impliquant plusieurs algorithmes de PQC, comme les signatures numériques.

ÉTUDE DE CAS

Une agence fédérale chargée de la sécurisation des réseaux critiques était particulièrement sensible à l'importance des performances et de l'interopérabilité lors de sa transition vers le PQC. Elle avait besoin d'un système prototype capable de fournir des résultats quantifiables de tests de performances et d'interopérabilité, incluant les impacts sur le matériel et les logiciels existants.

L'agence a utilisé un système de test pour quantifier les effets du PQC en simulant plusieurs connexions et en exécutant des scénarios de test faisant varier le trafic réseau, les contraintes de bande passante et les algorithmes utilisés tout au long de la connexion, lors des négociations d'authentification et de sécurité de la couche transport (TLS). Un tableau de bord visualisait automatiquement les résultats consultables. Cela a permis aux analystes de comprendre comment les négociations se feraient par défaut avec des algorithmes classiques lorsqu'un terminal n'était pas configuré pour le PQC ; d'identifier les effets des chaînes de certificats hybrides ; et de quantifier les coûts indirects et l'impact sur le réseau.

POINTS CLÉS À RETENIR

1. DÉVELOPPER DES ARCHITECTURES DE RÉFÉRENCE
   Déterminez où la cryptographie est utilisée dans un cas d'utilisation prioritaire pour définir l'implémentation du prototype, présenter les dépendances des fournisseurs et décrire les exigences d'interopérabilité.

2. ÉTABLIR UN TEST RÉUTILISABLE ENVIRONNEMENT
   Établir un environnement de laboratoire capable de simuler des solutions PQC hybrides et complètes pour déterminer la sélection et la mise en œuvre optimales des algorithmes.

3. CONCEVOIR UN PROTOTYPE PQC Évaluer les limitations matérielles et logicielles, les impacts sur les performances et l'interopérabilité dans le cas d'utilisation identifié.

Machine Translated by Google

Agilité cryptographique : optimisation pour une sécurité continue

Depuis les années 1970, les algorithmes à clé publique sécurisent nos vies numériques. Ces protections discrètes sont profondément ancrées dans le matériel, les logiciels et les protocoles numériques. Cependant, l'agilité et la gouvernance n'étaient pas intégrées aux décisions de conception relatives à la mise en œuvre de la cryptographie. Les fournisseurs de matériel ont intégré la cryptographie de manière à empêcher souvent toute mise à jour sans remplacer une puce entière. Les éditeurs de logiciels n'ont pas suivi la cryptographie à travers les différentes couches de leurs applications. Ces fournisseurs n'imaginaient pas un avenir où les mathématiques sous-jacentes à chaque algorithme cryptographique à clé publique seraient vulnérables aux attaques. Or, telle est la réalité actuelle, et elle oblige les entreprises à adopter de nouvelles normes PQC.

Les normes PQC initiales du NIST (publiées en août 2024) constituent la meilleure approche disponible pour se défendre contre la menace quantique. Cependant, il est possible que les avancées technologiques futures rendent ces normes vulnérables aux attaques. Il est également possible que de nouvelles normes PQC à venir offrent des performances supérieures aux normes initiales du NIST.

C'est là qu'intervient l'agilité cryptographique. Elle désigne la capacité à trouver, surveiller, mettre à jour et remplacer rapidement les cryptogrammes. Elle permet à une entreprise de s'adapter aux évolutions cryptographiques futures. Cette agilité est essentielle pour la PQC, mais son importance dépasse la cybersécurité post-quantique. Mises en œuvre de manière proactive et en harmonie avec d'autres priorités de modernisation de la cybersécurité, les stratégies de PQC qui privilégient l'agilité peuvent accroître l'efficacité et l'efficience globales des décisions d'approvisionnement des organisations.

ÉTUDE DE CAS

Un client du secteur de la défense a reconnu la nécessité d'investir très tôt dans la PQC afin de protéger son infrastructure lors de missions à fort impact. Il transformait déjà des opérations cybernétiques de plus grande envergure dans des domaines tels que le Zero Trust et la modernisation cryptographique, mais il savait que ces initiatives ne répondaient pas aux besoins en PQC. Ces efforts plus importants peuvent impliquer l'achat de nouveaux équipements coûteux et durables, tels que des radios tactiques et des chiffreurs. La simplification de ces décisions pour intégrer les considérations PQC permettrait d'accroître l'efficacité et l'efficience de leurs achats à long terme, de réduire les achats inutiles et d'éviter la dépendance à des fournisseurs qui ne se préparaient pas activement à la transition PQC. L'entreprise devait élaborer un plan d'agilité cryptographique.

En réunissant les parties prenantes internes et externes, l'agence a catalogué les dépendances cryptographiques entre les fournisseurs et les équipements existants ; surveillé les implémentations cryptographiques existantes, nouvelles et potentielles ; et inventorié les options de remplacement pour les capacités qui ne pouvaient pas prendre en charge les algorithmes PQC.

POINTS CLÉS À RETENIR

1. INTÉGRER PQC DANS MODERNISATION CONTINUE DE LA CYBERSÉCURITÉ

   Définissez comment PQC s'aligne sur les futures architectures de sécurité pour réduire la dette technique future et permettre une adoption rapide.

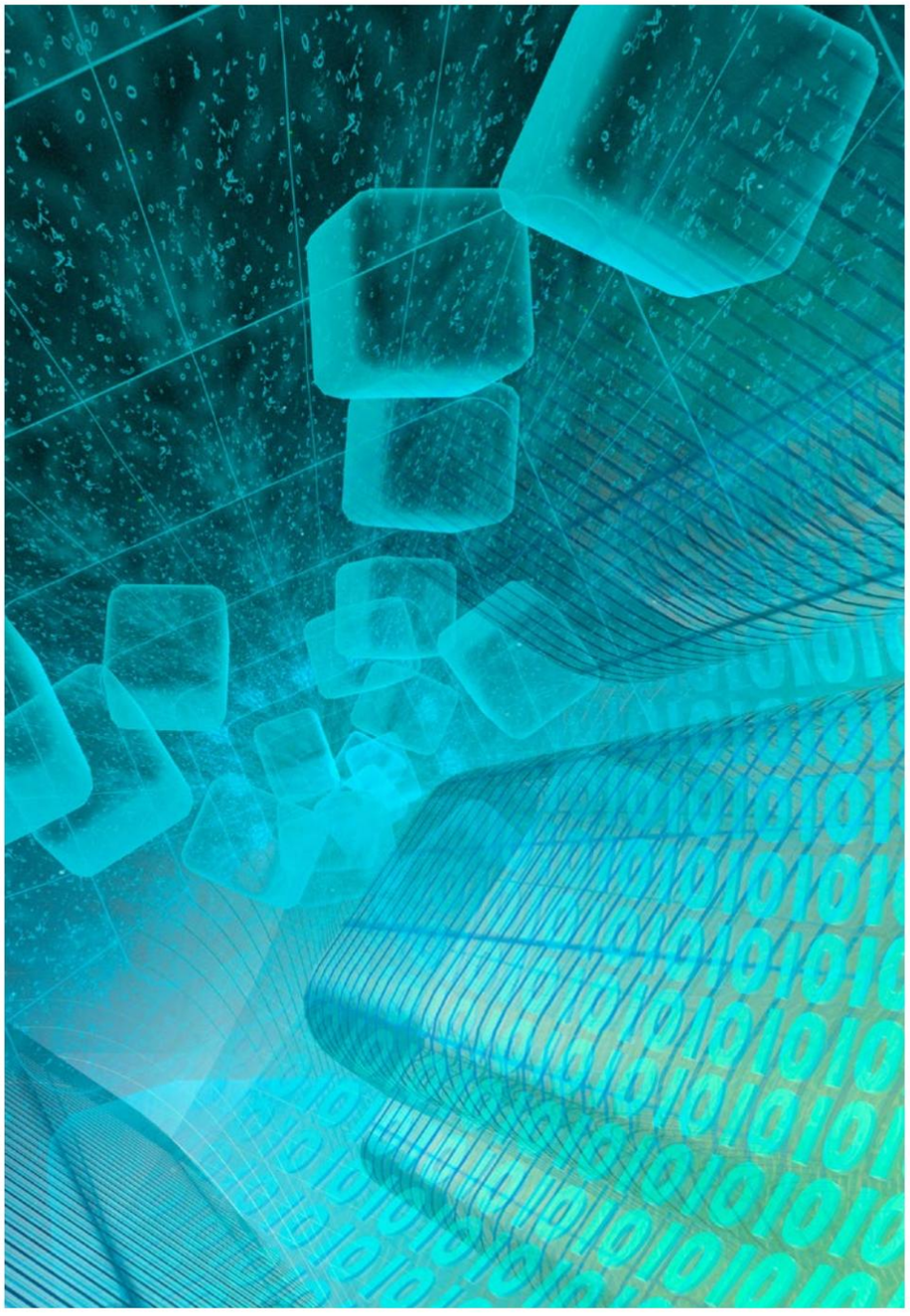
2. ÉNUMÉRER LES IMPACTS SUR LES ACHATS ET LES POLITIQUES

   Faites du PQC une priorité auprès des fournisseurs pour éviter le verrouillage avec des produits qui ne disposent pas de plans de transition PQC.

3. ÉTABLIR DES STRATÉGIES DE GESTION DES INFRASTRUCTURES ET D'APPLICATION DES POLITIQUES

   Permettre le transfert de connaissances pour renforcer la gouvernance tout au long de la transition.

Machine Translated by Google



Il n'y a pas de mauvais endroit pour Commencez la transition urgente vers le PQC

La voie vers la PQC peut être flexible, mais il s'agit d'une défense essentielle qui ne peut être ignorée. Chaque entreprise peut adapter son approche pour faire face aux vecteurs de menaces prioritaires. Ces études de cas illustrent les principaux effets observés par les organisations lors de leurs migrations à ce jour. Pour certaines, l'objectif initial était de combler le manque de capacités leur permettant de quantifier leur surface d'attaque quantique (encourageant ainsi la découverte cryptographique).

Pour d'autres, la possibilité que des tests de performance et d'interopérabilité insuffisants puissent entraîner des pannes de réseau dans des environnements critiques était évoquée (incitant au prototypage PQC). D'autres encore ont reconnu que l'absence d'intégration du PQC dans les initiatives en cours pourrait coûter des millions (incitant à l'agilité cryptographique).

Les responsables de la cybersécurité bénéficient d'une grande latitude quant à la manière dont ils démarrent leur parcours PQC, mais les organisations doivent commencer dès maintenant à se défendre contre les adversaires avancés en matière de cybersécurité et les menaces en constante évolution.

Taylor Brady dirige les engagements et les investissements de Booz Allen en matière de cryptographie post-quantique, se spécialisant dans l'adoption technique et le développement commercial.

Jordan Kenyon dirige la croissance et les opérations du portefeuille de technologies quantiques de Booz Allen, qui se concentre sur les nouveaux paradigmes que le quantique introduit pour l'informatique, la détection et les communications.

Derek Aucoin dirige le développement de produits et d'applications sécurisés pour la pratique commerciale mondiale de Booz Allen.

LECTURE RAPIDE

Les RSSI doivent concevoir des feuilles de route de transition PQC uniques qui s'alignent sur la surface d'attaque et les vecteurs de menace de leur agence.

Les entreprises peuvent éviter des coûts d'infrastructure supplémentaires et augmenter la vitesse de résolution en extrayant des données cryptographiques des capteurs réseau existants et en analysant ces données de manière innovante pour permettre la migration PQC.

L'intégration des plans de transition PQC aux autres efforts de modernisation de la cybersécurité est essentielle pour éviter le blocage des fournisseurs avec des solutions qui ne se préparent pas activement à la transition PQC.

Machine Translated by Google

MISSION À L'HONNEUR : DÉFENSE

Reconstruire le
Cycle de vie des missions tactiques

LA BOÎTE À OUTILS ÉMERGENTE POUR LES MODERNES

PLANIFICATION, PRÉPARATION ET PERFORMANCE

Cameron Mayer, Eric Syphard et Todd Burnett

Machine Translated by Google

Bien avant que les bottes des combattants ne touchent le sol ou que les avions prennent leur envol, certaines des actions militaires les plus importantes se déroulent loin du champ de bataille.

Aujourd'hui, les commandants américains consacrent beaucoup de temps et de ressources à la planification des opérations et à la formation du personnel aux situations auxquelles ils seront confrontés. Cette préparation est essentielle au succès des missions. Elle est également coûteuse, chronophage et insuffisamment approfondie en raison d'environnements d'entraînement sur le terrain irréalistes et des obstacles à l'intégration des données nécessaires à l'amélioration des performances des unités.

Accélérer la préparation des forces armées américaines nécessite une approche plus efficace et efficiente de la planification des missions. Utilisées conjointement, l'intelligence artificielle générative (GenAI) et les technologies de jumeaux numériques peuvent réinventer l'ensemble du cycle de vie des missions tactiques, de la planification et de la répétition à l'analyse après action. Les jumeaux numériques permettent aux combattants de s'entraîner et de répéter des actions dans des environnements virtuels réalistes. GenAI améliore le processus de planification en analysant rapidement les paramètres d'une mission par rapport à son objectif et à d'autres informations, et en générant et évaluant des plans d'action optimisés pour chaque point de décision clé. En résumé, le volant d'inertie moderne (voir l'article de couverture page 32) peut être appliqué ici pour accélérer la préparation des forces armées américaines.

Le résultat : les combattants peuvent simuler et s'entraîner à d'innombrables scénarios qu'ils pourraient rencontrer sur le champ de bataille, ce qui les rend mieux préparés aux niveaux stratégique, opérationnel et tactique pour exécuter des missions de manière sûre et efficace.

L'avantage : la planification et la formation dans un environnement virtuel sont efficaces en termes de temps et de coûts, car elles peuvent être effectuées là où c'est nécessaire, réduisant ainsi le temps de déplacement et avec moins de ressources, telles que l'équipement et les munitions.

Les couches d'un numérique Environnement de planification de mission

Un environnement numérique de planification de mission est construit à partir de vastes quantités de données provenant de l'environnement opérationnel, des combattants eux-mêmes et de la doctrine militaire. Le fondement est un jumeau numérique : une réplique virtuelle techniquement exacte d'un objet, d'un processus ou d'un système (pour en savoir plus sur les jumeaux numériques, voir page 34). Un jumeau numérique peut être créé en quelques heures à partir de données collectées via des cartes existantes et des survols de drones, grâce à des vidéos animées et à des balayages de détection et de télémétrie par lumière. Le résultat est un rendu haute fidélité du lieu où se déroulera une mission militaire.

La couche suivante est celle des données, intégrées au jumeau numérique afin d'offrir une vision claire des variables clés et autres paramètres. Cela comprend les données utilisées pour créer le jumeau numérique, ainsi que celles intégrées au système concernant la doctrine militaire, l'état de préparation des combattants, l'armement, la météo, les données open source et le renseignement d'origine électromagnétique. L'analyse et la mesure s'effectuent dans la couche d'intégration grâce au déploiement d'outils d'IA et d'optimisation mathématique traditionnels. Par exemple, un modèle d'optimisation mathématique traditionnel pourrait déterminer l'itinéraire le plus rapide entre différents points.

A et B pour une unité de quatre personnes transportant un ensemble défini d'équipements. Les modèles d'IA pourraient analyser le terrain en utilisant les catégories du OAKOC de l'armée : obstacles, voies d'approche, terrain clé, observation et champs de tir, et couverture et dissimulation.

En plus de reproduire l'environnement de la mission, les jumeaux numériques peuvent générer des données dépassant celles captées par les capteurs des drones. Un jumeau numérique peut être programmé pour simuler différentes conditions météorologiques, scénarios de combat et autres variables. L'intérêt de cette simulation est double : les combattants peuvent se tester et évaluer leurs performances dans diverses conditions, et les outils d'optimisation de l'IA peuvent s'entraîner sur ces données supplémentaires pour améliorer leurs fonctionnalités. (Pour en savoir plus sur la nature récursive de l'IA, consultez notre article « Tech à pleine vitesse ».)

Améliorer l'analyse et les connaissances humaines

L'introduction d'un assistant GenAI transforme un environnement de planification de mission numérique en une capacité de nouvelle génération. Un modèle GenAI va au-delà de la prédiction de résultats : il génère du contenu et des informations inédits. Il peut exploiter les informations et les schémas issus d'ensembles de données incroyablement volumineux pour non seulement recommander la meilleure ligne de conduite, mais aussi ajuster cette recommandation en fonction de variables supplémentaires et des retours d'information fournis en temps réel par le commandant. Pour la planification de mission, un modèle GenAI fondamental, entraîné à partir d'informations open source, est enrichi d'informations spécifiques à la mission, non accessibles au public, telles que la doctrine et les procédures militaires, les spécifications des uniformes et des équipements, les tactiques de combat typiques de l'adversaire et des informations classifiées spécifiques à la mission.

GenAI peut également surveiller les performances individuelles des combattants. Aujourd'hui, ces derniers peuvent être équipés de technologies portables qui génèrent des informations sur leur rythme cardiaque, leur respiration, leurs habitudes de sommeil, leur niveau de stress, leur posture, leur vitesse de déplacement, la longueur de leurs foulées et d'autres paramètres. Ces données biométriques fournissent des évaluations essentielles de leur état de préparation physique et mentale, qui peuvent être combinées à un hologramme tridimensionnel de chaque combattant dans un affichage incluant également des modèles d'équipement tactique et des informations sur le terrain à traverser. Sur cet affichage, les planificateurs peuvent glisser-déposer différents équipements sur les combattants afin de garantir que chacun puisse gérer efficacement la charge qui lui est assignée. Cela permet d'augmenter la vitesse globale pendant la mission, car une unité ne peut se déplacer qu'à la vitesse de son individu le plus lent.

Un logiciel d'orchestration utilisant l'IA agentique est le moteur du fonctionnement (pour en savoir plus sur l'IA agentique, voir page 41). Lorsqu'un commandant saisit une requête, un agent orchestrateur « commandant » l'interprète et assigne des tâches à des agents subordonnés. Chaque agent consulte ses procédures militaires principales pour identifier les étapes appropriées pour répondre à la question. Ensuite, en fonction des outils d'analyse disponibles, les agents exécutent chaque étape séquentielle.

Machine Translated by Google

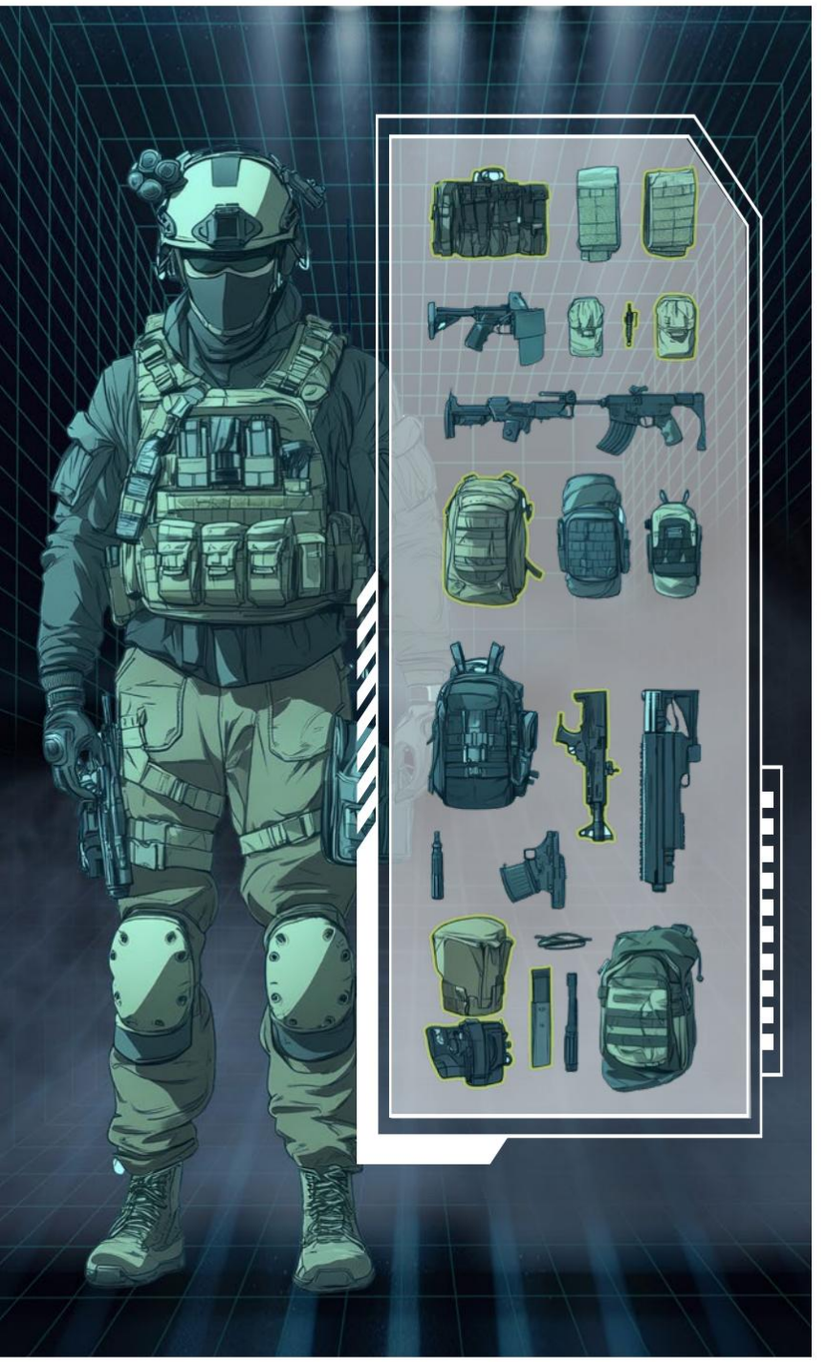


Figure 1 : Les jumeaux numériques permettent aux commandants de gérer la charge de chaque combattant.

ou notez une lacune dans les données ou les capacités disponibles avant de renvoyer une réponse à l'agent « commandant » pour examen, consolidation et réponse à l'utilisateur.

Chaque étape de cette séquence est enregistrée et mise à la disposition de l'utilisateur pour qu'il puisse l'examiner afin de garantir la transparence et l'auditabilité et de fournir un contrôle qualité contre toute « hallucination » potentielle générée par l'IA qui pourrait avoir un effet négatif sur l'opération.

Il est important de noter que cette approche ne prive pas le commandant de la prise de décision. Au contraire, elle lui fournit davantage d'outils de travail et de ressources.

Des données sur lesquelles le commandant peut s'appuyer pour appliquer son expérience, ses connaissances et son jugement afin de prendre de meilleures décisions. De plus, les humains doivent examiner les recommandations en tenant compte des principes éthiques, des nuances situationnelles et des conditions réelles, qui peuvent dépasser la compréhension des modèles d'IA actuels, et s'appuyer plutôt sur leur expérience et leur expertise.

Répétez pendant que vous combattez

La réalisation d'exercices de répétition constitue l'étape suivante du cycle de planification d'une mission. Les exercices centrés sur des modèles de terrain et des cartes unidimensionnelles demandent aux participants d'imaginer qu'ils se trouvent dans un endroit inconnu, devinant la pente d'une colline ou la densité d'une jungle. Même les modèles de terrain numériques classiques manquent de fidélité à la réalité, limitant la capacité des participants à visualiser le terrain et les conditions auxquelles ils seront confrontés. De plus, ils n'intègrent pas d'autres informations essentielles, comme la météo et les menaces potentielles.

Grâce au jumeau numérique, les combattants peuvent s'entraîner au combat, répétant le plan à plusieurs reprises dans un environnement simulé tridimensionnel réaliste, en immersion dans la zone d'opérations réelle. Ils peuvent visualiser le terrain, l'altitude, la végétation, les villages, les bâtiments : tout ce qu'ils rencontreront. La mission peut être répétée 10 ou 100 fois avant le départ, incluant le déroulement de l'action, l'évacuation médicale, la récupération des véhicules et les plans de capture de l'ennemi.

GenAI peut modifier dynamiquement le scénario au fur et à mesure que les combattants le parcourent, créant ainsi des défis nouveaux et inattendus. L'IA peut évaluer l'efficacité et la précision de l'activité opérationnelle ainsi que les systèmes physiques et psychologiques du combattant pendant l'action pour permettre un apprentissage et une préparation accrus.

Des systèmes électroniques sophistiqués permettent de combiner l'environnement simulé avec des armes réelles lors des répétitions de tir. Les soldats vivent une expérience virtuelle à 360 degrés tout en utilisant une arme de substitution offrant une expérience tactique et kinesthésique réaliste. Le système électronique comprend un microprocesseur qui collecte les données des capteurs de l'arme, comme la détente et la sécurité, et un gyroscope qui agit comme un capteur de mouvement et suit les mouvements de l'arme.

Lors des simulations présentées au soldat, ses actions et ses performances sont représentées sur un écran. Il peut visualiser la cible à travers l'optique de son arme, mesurer la portée, effectuer le tir, ressentir le recul et évaluer les dégâts. Ce type d'exercice de répétition robuste en réalité mixte, dans un environnement virtuel, permet aux soldats de répéter l'appel au feu encore et encore, de développer la mémoire musculaire nécessaire et d'apprendre à contrôler leurs émotions et à rester calmes dans des situations stressantes. L'IA peut identifier les facteurs à l'origine d'un échec d'appel au feu, comme les erreurs liées au stress ou au manque d'entraînement, offrant ainsi à chaque combattant et à son commandant un aperçu en temps réel des freins à leur performance et des solutions pour y remédier.

Machine Translated by Google

Perspective de l'industrie : Révéler

Reveal est une société leader dans le domaine de l'analyse visuelle et de l'IA de pointe, qui s'engage à aider le personnel de la défense et de la sécurité publique à atteindre la domination décisionnelle à la pointe de la tactique. Le vice-président de la Défense et de la Sécurité, Dave Caudle, a partagé son point de vue sur ces technologies et leur rôle dans les opérations militaires.

Vous êtes un ancien officier de l'armée américaine, actuellement commandant de bataillon dans la Garde nationale américaine et technologue. Comment l'IA va-t-elle transformer les opérations militaires à l'avenir ?

Je vois l'IA devenir un élément essentiel de l'état-major de combat. Cette technologie excelle dans le traitement et l'analyse des données, ce qui en fait une solution idéale pour améliorer la connaissance situationnelle des chefs d'escouade et de section en première ligne. L'emporter au combat repose souvent sur la capacité à prendre des décisions éclairées plus rapidement que l'adversaire. Il est essentiel de comprendre où déplacer ses forces et le chemin optimal pour y parvenir. Parfois, une décision aussi simple que le meilleur endroit pour atterrir un hélicoptère peut avoir des conséquences considérables. Les drones (UAS) peuvent collecter toutes sortes de données sur les conditions, et l'IA peut les analyser et présenter au chef d'escouade plusieurs pistes possibles, ainsi que les avantages et les inconvénients de chacune.

Il s'agit d'un niveau de perspicacité que les dirigeants des domaines avancés n'ont jamais eu.

Quels sont les plus grands défis techniques liés à l'intégration de l'IA à la pointe de la tactique ?

Le défi est de s'assurer que le peloton Le chef d'escouade ou le chef d'escouade dispose d'une interface lui permettant de communiquer rapidement et efficacement avec l'IA. Ces algorithmes effectuent des analyses à un rythme effréné, mais tout cela est vain si la personne qui les reçoit ne peut pas accéder à ces analyses et les comprendre à la vitesse de la mission.

C'est pourquoi il est impératif de concevoir ces interfaces pour qu'elles soient aussi intuitives et faciles à utiliser que possible. possible car dans les situations de conflit, le peloton les dirigeants doivent pouvoir recevoir des informations visuellement afin de pouvoir demander une analyse supplémentaire à l'IA ou prendre une mesure suggérée.

Quel sera le facteur clé de la réussite sur le champ de bataille à l'avenir ? Cela me fait un peu mal au cœur de le dire, mais je pense que les formations futures les plus efficaces emploieront moins de soldats et de chars, et 10 à 100 fois plus de machines intelligentes. Cela peut paraître un peu tiré par les cheveux, mais tout ce que nous avons appris ces dernières années, c'est que la robotique et l'autonomie transforment fondamentalement la guerre.

À mon avis, les drones sont la nouvelle munition. Ils sont appelés à devenir omniprésents, et notre succès dépendra de notre capacité à les produire à grande échelle et à former nos combattants à leur utilisation efficace.

Réinventer la revue après action

Tous les plans changent au contact ; les analyses a posteriori des événements réels sont donc essentielles pour optimiser les performances futures. Les analyses a posteriori classiques se concentrent sur les observations personnelles des dirigeants et des participants concernant le fonctionnement et la performance des tâches par rapport au résultat escompté. Cela permet à chacun d'évaluer ce qui s'est produit et ce qui ne s'est pas produit, et pourquoi, ainsi que les mesures à prendre pour préserver les points forts et améliorer les points faibles afin de faire mieux la prochaine fois.

Les jumeaux numériques et GenAI intègrent des données incontestables aux analyses post-action. Les mesures de performance sont fusionnées avec l'assistant GenAI, qui recommande des modifications à l'itinéraire prévu pour accélérer l'atteinte de la cible. De même, les mesures d'analyse de mission et les données biométriques collectées lors des répétitions fournissent un aperçu des performances de l'unité et des individus, ainsi que des modifications à apporter pour améliorer le plan et l'exécution de la mission. Les mesures de performance peuvent inclure la précision de la formation des escouades, la vitesse de déplacement, ainsi que le niveau de stress et d'énergie individuel. Les données issues des objets connectés peuvent aider les commandants à affecter le bon soldat à la bonne mission en fonction des forces et aptitudes individuelles, par exemple en déterminant si une personne scrute naturellement l'environnement et serait donc un meilleur tireur qu'une personne qui ne se concentre que sur quelques mètres devant elle.

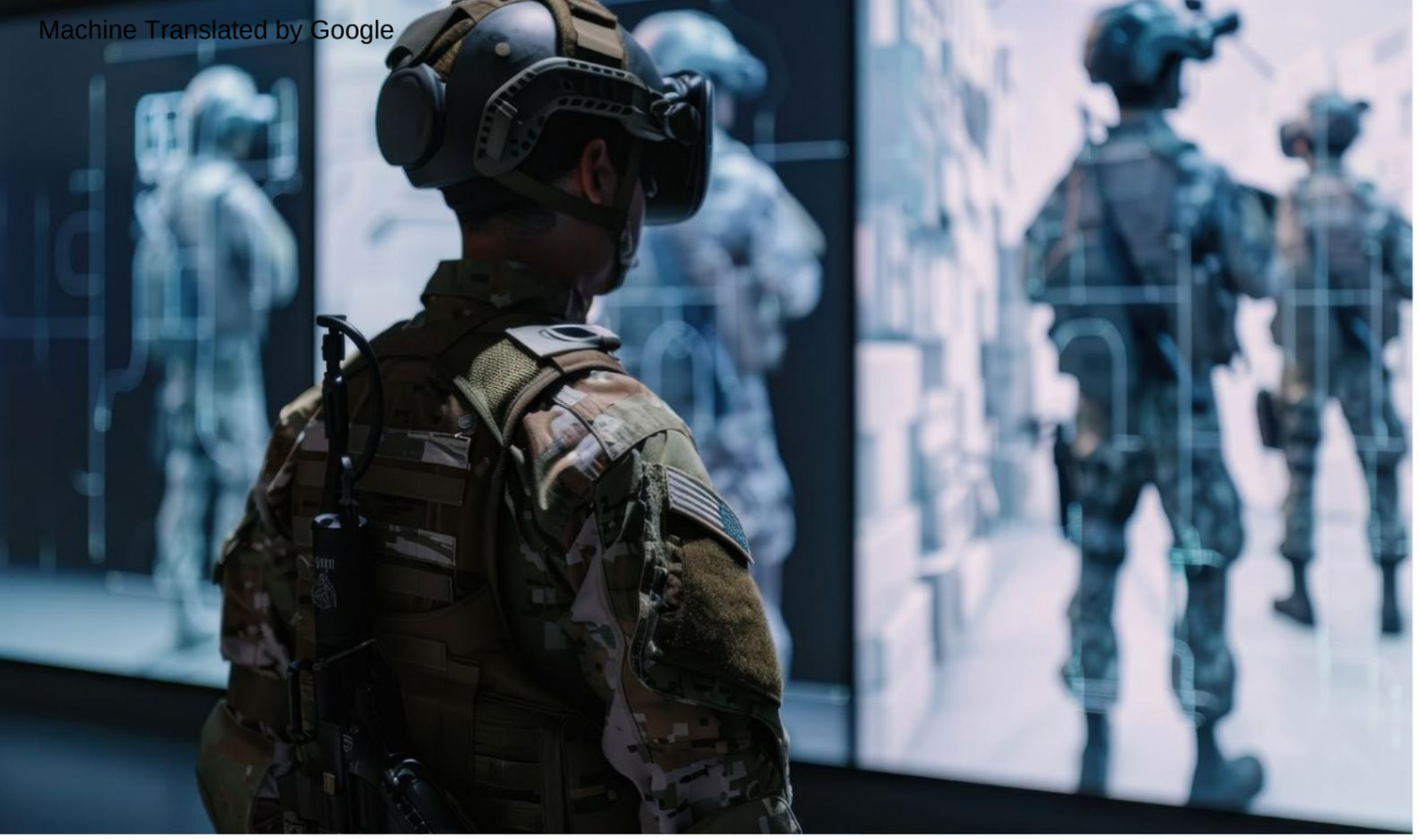
Une telle analyse a posteriori, basée sur les données, peut être réalisée après chaque répétition afin d'optimiser le plan. Lorsque la formation et les répétitions se déroulent dans un environnement numérique, les analyses et les révisions peuvent également être intégrées à l'exercice afin que les stagiaires puissent corriger leur trajectoire instantanément, ce qui n'est pas possible avec les exercices en présentiel.

Gratter la surface de ce qui est possible

La technologie GenAI est sur le point d'être utilisée en temps réel et quasi réel pour extraire en permanence de nouvelles données sur les menaces afin que les dirigeants puissent ajuster leurs décisions en fonction des informations actuelles et des recommandations mises à jour de GenAI. Associé à des jumeaux numériques, il peut considérablement améliorer la façon dont les combattants et les commandants militaires américains se préparent aux missions où la capacité à prendre des décisions éclairées dans des environnements imprévisibles est fondamentale pour le succès.

De plus, ces mêmes technologies peuvent être utilisées pour optimiser les chaînes d'approvisionnement et la logistique. Leur application à l'entraînement permet de gagner du temps et de réduire les coûts liés aux environnements réels, d'améliorer considérablement les taux de réussite et d'offrir aux combattants un plus grand soutien familial.

Machine Translated by Google



Le ministère de la Défense doit continuer à investir dans l'IA, car elle permet d'améliorer la prise de décision, tant au niveau tactique que stratégique.

Cameron Mayer dirige l'activité de préparation accélérée à la défense de l'entreprise en mettant l'accent sur la fourniture de solutions basées sur les données.

Eric Syphard dirige la pratique d'ingénierie IA du cabinet, qui se consacre à l'amélioration des performances des équipes homme-machine.

Todd Burnett est le conseiller exécutif principal de l'entreprise pour la préparation accélérée, axé sur la fourniture de solutions pour la formation et la préparation des combattants.

« Je pense que les formations futures les plus efficaces emploieront moins de soldats et moins de chars et entre 10 et 100 fois plus de machines intelligentes. »

– Dave Caudle, vice-président de la sécurité et la défense chez Reveal

LECTURE RAPIDE

GenAI et les jumeaux numériques ont le potentiel de reconstruire le cycle de vie d'une mission tactique, depuis la planification et la répétition initiales jusqu'à l'examen après action.

Les jumeaux numériques permettent des répétitions de mission réalistes dans des environnements 3D immersifs, permettant aux combattants de pratiquer et d'affiner leurs plans à l'aide d'analyses de performances en temps réel.

Les agents GenAI formés sur des informations spécifiques à la mission peuvent modifier dynamiquement les exercices de répétition, identifier les facteurs qui entravent les performances et fournir aux combattants des informations en temps réel sur la manière de les surmonter.

Systèmes intelligents à la périphérie

OBTENIR UN AVANTAGE DÉCISIONNEL DANS ENVIRONNEMENTS IMPRÉVISIBLES

Joel Dillon, Randy Yamada et Josh Conway

Concept de systèmes autonomes fonctionnant de manière indépendante

L'autonomie tactique décrit la

selon des paramètres définis pour exécuter des actions tactiques en conditions réelles. Ce concept est appelé à transformer les opérations militaires américaines dans tous les domaines, de la logistique dans le Pacifique à la surveillance derrière les lignes ennemies, en passant par la recherche et le sauvetage au combat. Il exigera également une refonte de la manière dont le Pentagone achète et déploie l'un des éléments fondamentaux de la technologie : les logiciels.

L'impact des plateformes de combat autonomes, telles que les programmes Replicator et Collaborative Combat Aircraft du ministère de la Défense (DOD), correspondra à la capacité de l'armée à fournir des mises à jour fréquentes et immédiates des logiciels et des algorithmes sous-jacents des plateformes.

Les ennemis du futur adapteront leurs armes et leurs tactiques, dissimulés sous un voile de camouflage et de tromperie, sous le brouillard de la guerre. Par conséquent, les plateformes autonomes auront besoin de renseignements nouveaux et de nouvelles capacités pour distinguer leurs alliés de leurs ennemis, évoluer en terrain inconnu, trouver et traquer leurs adversaires, et bien plus encore.

Le domaine naissant de l'autonomie tactique repose sur la gestion des données pour entraîner l'IA sous-jacente, mettre à jour les signatures et dicter les actions.

La préparation aux missions dans ce nouveau paradigme exige une collaboration plus étroite entre le Pentagone et le secteur privé, principale source d'innovation technologique du pays. Cela offrira également au Département de la Défense des opportunités d'acquérir et de maintenir des logiciels, des capteurs modulaires et d'autres matériels de manière innovante, ouvrant ainsi la voie à de nouvelles possibilités.

nouveaux entrants sur le marché et diversification de la base industrielle de défense américaine.

Les avantages de la fonctionnalité et de l'évolutivité

Les plateformes autonomes assureront diverses fonctions sur le champ de bataille, allant du renseignement, de la surveillance et de la reconnaissance (ISR) au soutien au combat rapproché, en passant par les relais de communication. Elles seront flexibles et adaptables : un seul véhicule autonome sans pilote (UAV) pourra entreprendre diverses missions au fil des jours. Elles seront « attractives » : conçues pour privilégier la fonctionnalité et la flexibilité plutôt que la durabilité. De plus, elles fonctionneront ensemble comme des systèmes intelligents, collaborant tactiquement avec une intervention humaine minimale.

L'un des principaux avantages des plateformes autonomes est qu'elles nécessiteront des débits de transmission de données inférieurs à ceux des véhicules pilotés à distance, ce qui leur permettra de fonctionner pendant de longues périodes. dans des environnements de communication austères, dégradés ou refusés.

Alors qu'un drone télécommandé doit pouvoir transmettre des vidéos à son pilote, un système ISR autonome peut se piloter lui-même ; il lui suffit de renvoyer les coordonnées d'une cible et la probabilité de réussite de son identification, par exemple. La réduction des besoins de communication allège les contraintes de latence des données, la complexité des messages et leur exploitabilité, nécessitant moins d'énergie et permettant un codage avancé et résistant au brouillage.

Conçus pour attaquer les lignes ennemies, les avions auront une durée de vie bien plus courte que les plateformes habitées actuelles, ce qui se traduira par un nouveau modèle de budget et d'infrastructure de soutien. Cette évolution est déjà en cours : l'armée de l'air a retiré du service le drone MQ-1 Predator d'origine moins de 15 ans après sa mise en service initiale, alors que de nombreux avions habités volent depuis plusieurs décennies.

Machine Translated by Google

Figure 1 : Cas d'utilisation de l'autonomie

Catégorie	Description
Renseignement, surveillance et Reconnaissance (ISR)	Les véhicules aériens, terrestres et maritimes sans pilote étendent la surveillance pour recueillir des renseignements sur le champ de bataille, distribuer des capteurs pour la collecte de données en temps réel et suivre les activités des véhicules et des unités.
Soutien au combat rapproché	Des drones hautement maniables, capables de voler à basse altitude et de mener des tactiques de précision, aident les troupes au sol, effectuent des frappes aériennes de précision et coordonnent des attaques en essaim qui submergent la cible.
Mine et explosif improvisé Guerre des engins explosifs improvisés (EEI)	Les véhicules sans pilote utilisent des capteurs pour localiser et neutraliser les engins explosifs improvisés et les mines navales.
Soutien médical	Des véhicules sans pilote plus petits transportent des médicaments et du matériel ; des véhicules plus grands équipés de systèmes robotisés fournissent des soins médicaux et transportent le personnel blessé.
Protection et sécurité des actifs	Les drones et les robots fournissent des services d'escorte pour les convois de grande valeur et gardent les installations clés.
Appui-feu et ciblage	Les plates-formes identifient les positions ennemies, fournissent des coordonnées aux unités d'artillerie et évaluent l'efficacité des engagements.

Un logiciel aussi dynamique que la mission

Tout au long de l'histoire, les ajustements apportés aux tactiques, techniques et procédures se sont transmis par des voies humaines, de la chaîne de commandement au soldat dans les tranchées ou au pilote dans le cockpit. Les chefs de mission déterminaient les charges de combat en fonction des besoins opérationnels immédiats, et un fantassin n'avait besoin d'aucune formation supplémentaire pour porter une charge lors d'une patrouille débarquée de plusieurs jours un jour et d'un engagement interarmes le lendemain.

Désormais, les plateformes autonomes s'appuieront sur une vaste bibliothèque de logiciels et d'algorithmes spécifiques à chaque mission. De même que les soldats ne peuvent transporter qu'une quantité limitée de matériel, les contraintes de taille, de poids, de puissance et de coût (SWAP-C) imposées aux capacités de stockage et de calcul d'une plateforme autonome limitent sa charge de combat aux algorithmes, logiciels et données nécessaires à la mission. Concrètement, cela se traduit.

est-ce qu'une mission impliquant une frappe cinétique nécessitera une charge utile logicielle différente de celle d'une évacuation médicale. D'autres téléchargements gourmands en données et en calcul pourraient être des systèmes de reconnaissance linguistique (par exemple, les panneaux de signalisation cyrilliques par rapport au cantonais) et la navigation sur le terrain dans des environnements sans GPS (par exemple, un actif déployé en Afrique de l'Est n'aura pas besoin de cartes détaillées de la province côtière du Guangdong), ou des algorithmes de vision par ordinateur pour la reconnaissance de cibles. Le Pentagone devra développer et améliorer en permanence les procédures permettant de mettre à jour la flotte.

Les limites du SWAP-C nécessitent également des opérations d'apprentissage automatique (MLOps) sophistiquées pour distinguer les renseignements du bruit. Ceci est particulièrement crucial pour les missions de longue durée dans des zones sans communication, comme les drones sous-marins opérant à proximité des côtes adverses. Ces véhicules sous-marins doivent fonctionner de manière autonome pendant de longues périodes.

Ils nécessitent des algorithmes avancés pour affiner les données collectées : distinguer les caractéristiques environnementales non pertinentes (par exemple, des images de mer déserte) des objets d'intérêt militaire (par exemple, des navires, des sous-marins, des mines). L'affinement des données réduit la capacité de stockage requise par les véhicules autonomes.

Une fois leur mission terminée, ces drones peuvent refaire surface à des emplacements prédéterminés pour transmettre rapidement les données pertinentes à des systèmes cloud sécurisés. Une gamme de modules matériels enfichables offrira une grande polyvalence, avec notamment différents ensembles d'ailes pour l'ISR en vol stationnaire ou l'attaque au sol, et différentes charges pour la guerre électronique ou une frappe cinétique. L'évolution des plateformes autonomes polyvalentes encouragera également l'innovation en matière de matériel et de capteurs.

L'histoire récente de la guerre offre d'innombrables exemples de mises à jour tactiques qui n'auraient pas pu être prévues avant le déploiement d'une plateforme sur le terrain.

Le logiciel nécessite des mises à jour pour être optimisé

Machine Translated by Google

Performances, même dans des environnements relativement statiques. Les environnements permissifs et collaboratifs pour systèmes complexes, tels que les voitures autonomes, peuvent nécessiter des mises à jour fréquentes pour améliorer la sécurité et l'expérience de conduite. Le monde concurrentiel de l'espace de combat moderne, avec un adversaire en constante évolution, accroît ce besoin de manière exponentielle. Des nouvelles armes, capteurs et signatures adverses aux tactiques perfectionnées, un comportement optimal nécessitera le déploiement quotidien, voire horaire, de mises à jour logicielles.

Le défi de l'intégration Les défis techniques, logistiques et bureaucratiques pour apporter de l'autonomie aux opérations militaires, et bientôt, exigent une intégration sans précédent du matériel, des logiciels, des algorithmes et des équipes humaines, tant au niveau de l'entreprise qu'à la périphérie.

Les opérations militaires autonomes seront constituées d'une multitude de plateformes autonomes et de systèmes d'entreprise. Les mises à jour sur une plateforme devront être coordonnées et synchronisées à travers l'ensemble du système. Un sous-marin et un avion autonomes proviendront de fabricants différents, mais devront collaborer : l'un détectera les mines tandis que l'autre assurera la surveillance aérienne.

Les systèmes intelligents composés de multiples plateformes autonomes exigeront des données et des capacités de calcul de niveau hyperscale. L'infrastructure logistique nécessaire au transfert de l'ensemble des données et des algorithmes doit être considérée comme un système de combat critique à part entière. Les données elles-mêmes constituent un atout stratégique ; dans son « Estimations budgétaires pour l'année fiscale 2025 », l'Agence des systèmes d'information de la Défense a souligné « le pouvoir inhérent à la possession de données pour contrôler les positions dominantes ». L'infrastructure de données et de communication nécessitera une protection cybernétique robuste.

Pour chaque scénario de mission et plateforme autonome les mettant en œuvre, les développeurs doivent créer, vérifier et valider les mises à jour. Leur diffusion sécurisée au sein de la flotte représente une immense complexité technique et logistique. Une future force devra mettre à jour simultanément des dizaines, voire des centaines de milliers, de systèmes sans pilote, ce qui pourrait engendrer un goulot d'étranglement considérable en matière de données. Imaginez les difficultés rencontrées par les supporters de football américain.

PERSPECTIVE DE L'INDUSTRIE :

IA du BOUCLIER

Nathan Michael est le directeur technique de Shield AI et ancien professeur associé de recherche à l'Institut de robotique de l'Université Carnegie Mellon.
Il est l'auteur de plus de 150 publications sur le contrôle, la perception et la cognition pour les systèmes d'IA mono et multi-robots.
Nous avons discuté avec Nathan de l'avenir des plateformes autonomes.

Vous avez mené des recherches sur l'intelligence collective. Pourriez-vous nous expliquer ce que c'est ?

L'intelligence collective consiste à créer des systèmes capables de répondre à des exigences de mission spécifiques dans des environnements variés. L'essaimage, notamment dans les environnements sans communication et sans GPS, en est un excellent exemple. Il implique la collaboration d'un grand nombre de systèmes hautement intelligents. Dans le pire des cas, en cas de perte de communication, chaque système est capable de fonctionner de manière indépendante. Une fois les communications rétablies, ils peuvent rétablir la coordination et collaborer pour atteindre les objectifs de la mission. En créant des équipes résilientes et adaptatives, capables de fonctionner dans différents ensembles de missions et domaines, nous évoluons vers l'essaimage : des systèmes hautement intelligents et performants fonctionnent ensemble avec efficacité et restent résilients, même dans des environnements conflictuels.

Quel est le plus grand défi à relever pour opérationnaliser l'autonomie dans des environnements réels ?

Le plus grand défi réside dans la mise à l'échelle de la production. De nombreux laboratoires de recherche et développement industriels et équipes universitaires développent déjà des capacités d'autonomie de mission efficaces. La question est de savoir comment construire des cadres de test de bout en bout pour la vérification, la validation et le déploiement ? Comment définir un concept d'usine bien défini permettant de multiplier la production et d'en étendre le déploiement ? La véritable innovation de la Model T ne résidait pas dans la voiture, mais dans la création d'usines capables de la produire en série. Nous sommes confrontés à un défi similaire : notre industrie doit dépasser la conception et la construction de capacités autonomes sur mesure, applicables à des scénarios spécifiques, pour adopter des processus permettant de construire des plateformes autonomes pour diverses applications de mission, à grande échelle et à grande vitesse.

À quoi ressemble l'avenir des systèmes autonomes ?
Actuellement, l'autonomie tactique concerne les systèmes exécutant des tâches spécifiques liées à une mission, comme l'ISR ou les frappes de précision, des opérations qui nécessitent traditionnellement une intervention humaine à tous les niveaux. Un exemple d'autonomie tactique serait un drone naviguant de manière autonome dans un environnement sans GPS pour mener une frappe ciblée. Cependant, l'autonomie stratégique ne se limite pas à l'exécution de tâches isolées. Elle signifie que les systèmes seront capables d'évaluer l'environnement opérationnel global, de prendre des décisions de haut niveau et d'adapter leurs objectifs à l'évolution de la mission. Par exemple, un système stratégiquement autonome pourrait coordonner plusieurs moyens, gérer une opération complexe dans différents domaines (aérien, terrestre, maritime) et ajuster les priorités de la mission en temps réel en fonction des conditions du champ de bataille. Cela permet à un personnel réduit de commander des effets plus importants avec plus de précision et d'efficacité.

Le passage de l'autonomie tactique à l'autonomie stratégique vise également à minimiser les risques pour le personnel tout en maximisant les résultats des missions. Avec moins de personnes en danger, des systèmes plus intelligents traiteront les données et prendront des décisions à grande échelle. Cette capacité cognitive accrue des plateformes autonomes permettra aux opérateurs de prendre de meilleures décisions avec moins de ressources, améliorant ainsi leur efficacité sur le champ de bataille. En bref, nous aurons besoin de moins d'humains pour atteindre des objectifs de mission bien plus ambitieux, tandis que les systèmes intelligents assumeront des rôles plus complexes et de haut niveau, autrefois réservés aux commandants humains.

Machine Translated by Google

Appareils mobiles dans le stade pendant un match. Cet effort nécessitera un routage avancé basé sur la périphérie pour déplacer les données sur le meilleur réseau disponible sans intervention humaine.

Un commandement de combat pourrait bientôt stocker 10 000 drones hors tension dans un entrepôt pendant des mois, en attendant un événement majeur. La force devrait mettre à jour et synchroniser ces engins le plus rapidement possible pour leur déploiement, y compris de nouveaux logiciels et algorithmes. Une voiture civile autonome peut effectuer plusieurs mises à jour par semaine dans un environnement de communication permissif. Les opérations militaires peuvent se dérouler dans des environnements contestés et non permissifs, où la connectivité nécessaire pour recevoir les mises à jour n'est pas toujours assurée.

Ce que le progrès exige

Un nouveau paradigme pour les opérations militaires exige un nouveau paradigme pour le développement et l'acquisition de logiciels. L'évolution vers des systèmes autonomes performants entraînera une transformation profonde de l'économie de la défense nationale, notamment par une réorientation du budget du Pentagone des opérations et de la maintenance conventionnelles vers les logiciels. Elle obligera également le DOD à repenser la gestion des données. Pour garantir l'amélioration continue des plateformes autonomes, il sera impératif de développer des capacités capables de collecter et de stocker un maximum de données dans des environnements d'entraînement permissifs et avec moins de contraintes réseau. Ces données permettront d'entraîner les algorithmes qui serviront de cerveau aux véhicules et armes autonomes.

Les modèles d'acquisition technologique du DOD ont été développés au fil des décennies pour s'adapter à l'achat de matériel informatique volumineux et coûteux ou de logiciels d'entreprise de grande envergure. Ces modèles d'acquisition devront être plus agiles et plus flexibles pour suivre l'évolution technologique.
Dans le cadre des modèles actuels d'approvisionnement, d'exploitation et de maintenance, le sous-traitant d'origine d'une plateforme est généralement chargé de la maintenance et de la mise à jour de son matériel et de ses logiciels.
Mais la start-up ou l'entreprise technologique qui a fabriqué un avion autonome n'est peut-être pas la mieux placée pour écrire des algorithmes spécifiques à une mission ; ses ingénieurs et ses dirigeants n'ont peut-être pas l'expérience nécessaire pour travailler avec des clients fédéraux ou les habilitations de sécurité pour comprendre pleinement la nature de l'opération.

Les fabricants d'équipements d'origine (OEM) bloquent généralement le financement du maintien en condition opérationnelle d'une plateforme sophistiquée et sophistiquée pendant les décennies de son exploitation. Les plateformes performantes à courte durée de vie nécessiteront moins de maintien en condition opérationnelle, mais des mises à jour logicielles fréquentes seront nécessaires. L'accès au marché des logiciels, plus facile que le développement et la fabrication, par exemple, d'un avion de chasse avec équipage, permettra à davantage d'entreprises de se lancer dans l'innovation, avec une efficacité et une résilience accrues de la chaîne d'approvisionnement. De plus, il n'est peut-être pas judicieux, d'un point de vue financier, pour chaque entreprise privée fabriquant des drones de haute qualité d'investir dans la personnalisation de ses produits pour les paramètres très spécifiques des opérations de défense.
Alors que l'autonomie devient de plus en plus essentielle à la défense de notre nation, Le DOD pourrait devoir conserver le contrôle des algorithmes qui régissent le comportement des systèmes autonomes. En séparant le code et en en étant propriétaire, le DOD peut acquérir les meilleurs drones et drones disponibles sans avoir à dépendre des fabricants pour adapter le produit aux spécificités de missions en constante évolution.

Dissocier l'acquisition de matériel et l'acquisition de logiciels permettra également au DOD d'acquérir les technologies les plus récentes et performantes auprès d'une base de fournisseurs élargie de la Silicon Valley, travaillant de concert avec les principaux sous-traitants de la défense. Imaginez un logiciel performant pour l'analyse post-mission, accessible à tous les escadrons utilisant des drones, quel que soit le fabricant du matériel. Les systèmes autonomes continueront d'évoluer et d'acquérir de nouvelles capacités, capables de répondre à diverses fonctions clés des missions.

Adopter une mentalité axée sur les logiciels aidera le DOD à se positionner pour mettre à profit les technologies les plus innovantes afin de relever les plus grands défis.

Joel Dillon est un leader du secteur de la défense mondiale de Booz Allen, qui pilote les technologies de nouvelle génération via l'activité Digital Battlespace de l'entreprise.

Randy Yamada, Ph.D., est un leader technique supervisant l'autonomie et les incarnations de l'IA physique pour le secteur de la défense mondiale de l'entreprise.

Josh Conway, Ph.D., développe la stratégie et la mise en œuvre de systèmes autonomes à grande échelle.

LECTURE RAPIDE

Pour déployer avec succès l'autonomie tactique dans les opérations militaires américaines, le Pentagone devra repenser la manière dont il achète et déploie l'un des éléments fondamentaux de la technologie : les logiciels.

Les plateformes autonomes s'appuieront sur une vaste bibliothèque de logiciels et d'algorithmes spécifiques à chaque mission et nécessiteront des mises à jour régulières en fonction des missions qu'elles sont censées exécuter.

La séparation de l'acquisition de matériel et de logiciels permettra également au DOD d'acheter les dernières et meilleures technologies auprès d'une base de fournisseurs élargie de la Silicon Valley travaillant de concert avec les principaux entrepreneurs de la défense.

Machine Translated by Google

MISSION À L'HONNEUR : LES FORCES DE L'ORDRE

Une autre paire d'yeux

DES OUTILS INTELLIGENTS POUR AMÉLIORER LE DROIT PERSONNEL D'APPLICATION DE LA LOI

Carl Ghattas, Todd Kline et Thong Nguyen

Machine Translated by Google

Les agents des forces de l'ordre (LEO) bénéficieront-ils lorsque certains aspects du costume « Iron Man » de Tony Stark deviendront viables dans des scénarios réels ? Comment

Les armures propulsées par fusée relèvent peut-être de la science-fiction, mais les capteurs corporels, le calcul neuronal à très faible consommation et les écrans de réalité augmentée (RA) haute résolution gagnent rapidement en puissance. Aujourd'hui, ces technologies sont disponibles dans des formats aussi compacts qu'une paire de lunettes. Demain, elles constitueront le fondement d'une plateforme permettant des capacités surhumaines sur le terrain.

La convergence de ces technologies avec l'IA donne naissance à un nouveau paradigme d'outils « intelligents » de terrain, capables d'offrir des fonctionnalités telles que la traduction active, l'orientation contextuelle ou la visualisation en temps réel des activités criminelles ou du soutien tactique à proximité. Intégrées à une plateforme portable simple et connectée à la 5G, ces technologies offrent aux forces de l'ordre la possibilité de voir l'invisible, de communiquer sans avoir à parler et de maintenir une connaissance situationnelle (CS) inégalée aujourd'hui.

Cependant, à l'instar des dispositifs de vision nocturne ou des caméras corporelles, dont l'adoption a pris des années, les avancées significatives des technologies embarquées sur le terrain ne se font pas du jour au lendemain. Avant que les dispositifs portables alimentés par l'IA ne migrent du laboratoire vers le terrain, les agences peuvent prendre certaines mesures pour se préparer et préparer leur personnel. Il est impératif de comprendre comment ces capacités peuvent s'adapter aux besoins des missions, les solutions à apporter avant leur déploiement opérationnel, et comment l'IA peut réduire la complexité et améliorer la connaissance de la sécurité pour les forces de l'ordre sur le terrain.

Noyé sous un tsunami de données

Aujourd'hui, les forces de l'ordre et les agents de sécurité intérieure sont confrontés à un défi quotidien : gérer les flux de données essentiels à leurs opérations quotidiennes. Ces données leur parviennent sous différents modes (images, publications sur les réseaux sociaux, informations) et proviennent de sources diverses (caméras-piétons, bases de données des forces de l'ordre). Elles sont souvent cloisonnées au sein des organisations et classées sous différentes classifications.
Selon un article publié par IT Brew, En juin 2024, Justin Williams, directeur adjoint adjoint de la division de gestion de l'information du FBI, a déclaré que la division des services d'information sur la justice pénale du bureau peut contenir plus de 30 pétaoctets de données à tout moment.

Les agences fédérales et les forces de l'ordre locales se tournent vers l'IA pour traduire ce déluge de données en informations. Selon IT Brew, Cynthia Kaiser, directrice adjointe adjointe de la division Cyber du FBI, a déclaré que le bureau avait utilisé le traitement du langage naturel pour analyser les appels d'information et identifier les informations manquantes. En août 2024, le bureau du shérif du comté de Palm Beach a annoncé à WPEC CBS 12 le déploiement d'un outil d'Axon Enterprise, Inc., qui utilise l'IA générative et les flux audio de caméras corporelles pour produire des brouillons de rapports d'incident. Ces cas d'utilisation permettent de gagner du temps tout en préservant la responsabilité humaine, essentielle pour garantir le respect par les agences des lois protégeant la vie privée et les droits des citoyens, et régissant l'admissibilité des preuves devant les tribunaux.

Ils évoquent également un avenir où l'IA peut aider les forces de l'ordre à mieux traiter des scénarios complexes et à réduire la charge cognitive sur le terrain.

Optimiser l'intelligence du bureau à la périphérie

Si les applications de l'IA dans les forces de l'ordre sont aujourd'hui principalement axées sur les tâches administratives, l'essor des appareils connectés ouvre de nouvelles perspectives. Comment cette technologie émergente pourrait-elle répondre aux besoins non satisfaits des forces de l'ordre sur le terrain, souvent éloignées des sources d'information et des centres de décision ? Comment l'IA portable pourrait-elle améliorer la sécurité des données, essentielle au succès des opérations sur le terrain ? En comblant l'écart entre les forces de l'ordre et les informations essentielles, cette technologie pourrait aboutir à une prise de décision distribuée et à une meilleure efficacité des réponses.

Pour les forces de l'ordre sur le terrain, la conscience de soi est un état nécessaire, mais difficile à atteindre. Elle peut facilement être altérée dans des situations de forte pression, où des décisions prises en une fraction de seconde peuvent faire la différence entre la vie et la mort. En situation de stress important, les forces de l'ordre doivent percevoir des signaux environnementaux tels que des menaces potentielles dans des environnements inconnus, comprendre leur signification dans le contexte (par exemple, faire la distinction entre une personne nerveuse et une personne agressive) et être capables d'anticiper des scénarios futurs à partir d'observations actuelles.

Développer une vision opérationnelle commune (COP) à partir d'une SA individuelle représente un défi encore plus complexe. Il implique la fusion en temps réel des informations provenant de sources individuelles et disparates afin de fournir une vue unifiée, tout en orchestrant la diffusion des informations pertinentes pour les missions spécifiques de chaque officier des forces de l'ordre. Cette complexité est décuplé dans les opérations multi-agences, où les intervenants peuvent être guidés par des mandats, des objectifs et des sources d'information différents, ce qui peut compliquer la collaboration. Dans les situations dynamiques et en constante évolution auxquelles sont confrontées les officier des forces de l'ordre sur le terrain, les erreurs de transmission d'informations critiques de manière pertinente et opportune peuvent avoir des conséquences désastreuses.

Malgré l' importance des technologies COP pour la sécurité publique, il n'est pas rare que ces systèmes ne bénéficient pas des fonctionnalités offertes par les technologies émergentes. Par exemple, les forces de l'ordre peuvent utiliser des moyens sophistiqués tels que des hélicoptères et des drones pour capturer des données visuelles précieuses. Le problème est qu'une fois ces informations reçues et traitées par le commandement central (C2), les informations qui en résultent sont souvent transmises au personnel de terrain verbalement plutôt que numériquement. De plus, le risque de latence et d'erreur augmente à mesure que l'information se propage à d'autres organisations.

Il existe des opportunités significatives pour créer des systèmes qui réinventent la circulation des données du terrain vers le bureau, puis vers d'autres agences, et inversement. Ces systèmes doivent contribuer à répartir le « bruit » et aider les forces de l'ordre à se concentrer sur l'essentiel. L'enjeu n'est pas toujours de trouver rapidement l'aiguille dans la botte de foin, mais plutôt d'éliminer efficacement le foin qui l'enveloppe.

Machine Translated by Google

Un aperçu du possible

Imaginez une paire de lunettes, d'apparence banale, mais spécialement conçues pour les forces de l'ordre en première ligne. Une fois activées et portées, elles authentifient biométriquement le porteur, lui offrant ainsi un accès sécurisé à des fonctionnalités avancées.
Des données de mission spécifiques, telles que des profils de suspects, des cartes, des plaques d'immatriculation ou des plans d'étage de bâtiments, leur sont transmises, permettant un fonctionnement hors ligne en cas de lacunes dans la couverture sans fil.

Grâce à un visuel net et large, le LEO voit les informations pertinentes à sa mission superposées dans son champ de vision.

Les données recueillies vont du guidage routier et de la circulation à la localisation des suspects et des membres de l'équipe. Les forces de l'ordre sont également alertées des menaces à proximité. Pendant une opération, les lunettes identifient visuellement les « amis ou les ennemis » à distance, réduisant ainsi les risques de tirs amis sur les autres forces de l'ordre, en service ou non. Les lunettes estiment également la taille et la densité de la foule, identifiant des caractéristiques clés telles que les schémas de mouvement.
La reconnaissance faciale est effectuée sur l'appareil par rapport aux profils suspects préchargés, réduisant ainsi les allers-retours inefficaces tout en protégeant la vie privée des citoyens respectueux des lois.
Une simple commande verbale incite les lunettes à capturer et à cataloguer numériquement les données ainsi que leur contexte environnant dans le temps et l'espace, des informations qui soutiennent les futures analyses médico-légales.

Grâce à ses capacités d'intelligence de scène embarquées, une paire de lunettes intelligentes alimentées par l'IA maintient en permanence une simulation spatio-temporelle du monde qui l'entoure.
Les lunettes transmettent au C2 les mises à jour delta de leur « compréhension du monde » local, qui sont fusionnées avec les données du système d'information géographique et d'autres sources, telles que les flux de drones et de télévision en circuit fermé (CCTV), pour créer un jumeau numérique centralisé et en direct de la zone de couverture. Cela fournit une vue unifiée, ainsi que des analyses historiques et des simulations prédictives pour soutenir les décisions basées sur les données. L'état central qui en résulte est régulièrement synchronisé avec les LEO pour fournir à chaque individu une vision en temps réel, comparable à celle d'un essaim.

Une fixation rapide d'un capteur supplémentaire permet aux lunettes de détecter au-delà du spectre visible, y compris la présence de matières chimiques, biologiques ou nucléaires, ce qui permet au LEO de voir et de signaler instantanément ses découvertes.
Tout cela se passe sans qu'un mot ne soit prononcé.

Les flux de données sous-jacents peuvent être capturés sous forme d'enregistrements historiques et seront d'une valeur inestimable non seulement pour les rapports après action, mais également pour la formation des nouvelles recrues et la synthèse des scénarios futurs qui ne se sont pas encore produits.

Outre l'assistance passive, les forces de l'ordre peuvent émettre des requêtes vocales actives, posant des questions et donnant des instructions telles que : Où a été observé le suspect pour la dernière fois ? Y a-t-il des civils dans la zone ? Obtenez-moi une vue aérienne de l'origine des appels au 911 liés à cet incident. Quel est l'itinéraire le plus rapide et le plus sûr pour sortir de la zone ? Grâce à leur compréhension des contextes individuels et collectifs, les lunettes peuvent fournir des réponses adaptées à la situation en quelques millisecondes. Des politiques et procédures à jour peuvent être demandées, ce qui peut être difficile à mémoriser pendant ou après des événements stressants.

La construction et le déploiement d'une telle plateforme relèvent du domaine du possible. Disponible commercialement.

Les lunettes intelligentes telles que la collection Ray-Ban Meta, Snap Spectacles ou DigiLens Argo™ sont dotées de capteurs électro-optiques haute résolution et d'un processeur Qualcomm Snapdragon® capable d'exécuter des modèles d'IA en parallèle avec une simulation physique complète à 60 images par seconde.

Elles disposent d'une connectivité sans fil permettant une faible latence pour accéder à une infrastructure sécurisée. Elles permettent déjà la conversion de la parole en texte, la synthèse vocale, la vision par ordinateur, le streaming vocal et vidéo. Les prochaines générations de lunettes offriront encore plus. Pour les rendre performantes, il faudra combiner harmonieusement les technologies sous-jacentes pour atteindre un objectif précis.

Dans le cadre des missions de maintien de l'ordre, qui couvrent l'ensemble des aspects de la sécurité publique, notamment la facilitation de la circulation légale des personnes et des biens, la perturbation des activités illicites ou l'investigation réactive d'innombrables informations et pistes, le principal défi réside dans la fusion et la diffusion des données, ainsi que dans l'expérience utilisateur. Toute information transmise à un agent des forces de l'ordre de première ligne doit le faire de manière à mettre en évidence le contexte pertinent et à éliminer les éléments parasites, sans pour autant constituer une distraction ni une charge cognitive.

Pour être efficace sur le terrain, cette plateforme devra respecter des limites strictes en termes de taille, de poids et de puissance. Les agents des forces de l'ordre ne porteront pas de lunettes fragiles, nécessitant des changements de piles fréquents ou attachées à des cordons limitant les mouvements.
De nombreuses forces de l'ordre sont déjà surchargées d'équipement : armes, caméras corporelles, matériel de premiers secours, éclairages, etc. Les mises à jour des appareils, des applications clientes, des microservices de cloud privé et de l'infrastructure correspondante doivent être fluides et évolutives à mesure que l'utilisation augmente, ce qui rend le « Software-Defined Everything » (SDE) indispensable. Sans une efficacité manifeste et sans faille, l'adoption sera difficile, voire impossible.

De plus, dans une situation d'urgence comme l'exécution d'un mandat ou la poursuite d'un suspect, les lunettes doivent pouvoir anticiper les besoins des forces de l'ordre. L'intégration de l'IA multimodale augmentera considérablement la proposition de valeur en soutenant directement l'exécution des tâches. Pour les missions de maintien de l'ordre, des lunettes exploitant les capacités analytiques avancées de l'IA pour identifier proactivement les exigences d'une situation spécifique…

Des informations sur la zone environnante, des demandes de renforts, plutôt que d'attendre uniquement des ordres verbaux, amélioreront la SA des forces de l'ordre et accéléreront la prise de décision dans les situations critiques.

Du laboratoire au terrain

Les discussions sur les technologies émergentes et leur pertinence potentielle pour les missions suscitent souvent l'enthousiasme, mais une véritable transformation des missions exige une approche bien plus nuancée et méthodique. Le paysage technologique regorge de concepts ratés, issus d'hypothèses erronées. Il est essentiel d'incuber et de développer ces produits en étroite collaboration avec les experts actuels des missions afin de garantir qu'ils répondent aux besoins pratiques et aux contraintes réelles du personnel de terrain. Les tests utilisateurs itératifs et le retour d'expérience sont essentiels pour instaurer la confiance, identifier et résoudre les problèmes potentiels, améliorer la convivialité et valider les fonctionnalités clés. L'utilisation de toute technologie d'augmentation humaine au service de la sécurité publique doit pouvoir s'adapter avec fluidité aux besoins des missions et résister aux exigences du terrain.

Machine Translated by Google

Deux événements à venir illustrent comment les objets connectés alimentés par l'IA pourraient aider les forces de l'ordre à surmonter leurs défis en matière de données : la Coupe du monde de la FIFA 2026™ et les Jeux olympiques d'été de 2028. Les États-Unis accueilleront les deux événements et, au cours de chacun d'eux, des dizaines de millions de fans et de touristes internationaux passionnés convergeront physiquement et numériquement en peu de temps, générant des milliards de dollars de revenus, créant des dizaines de milliards d'impressions et attirant une attention mondiale massive.

Ces spectateurs et touristes ne feront qu'ajouter au tsunami déjà croissant de données auquel les forces de l'ordre sont confrontées.
Mais au lieu d'une hausse généralisée, la nature limitée de ces événements focalisera cette augmentation de données de manière aussi aiguë que la pression de l'eau dans une lance à incendie. Pour enquêter efficacement sur toute piste, identifier et déjouer les activités illicites et faciliter la circulation sûre et légale des personnes, les forces de l'ordre devront disposer en permanence d'une capacité de surveillance aussi complète que possible.
Les outils intelligents utilisés sur le terrain pourraient-ils constituer le pont reliant ces missions infaillibles aux données nécessaires pour les exécuter avec succès quand et où cela est nécessaire ?

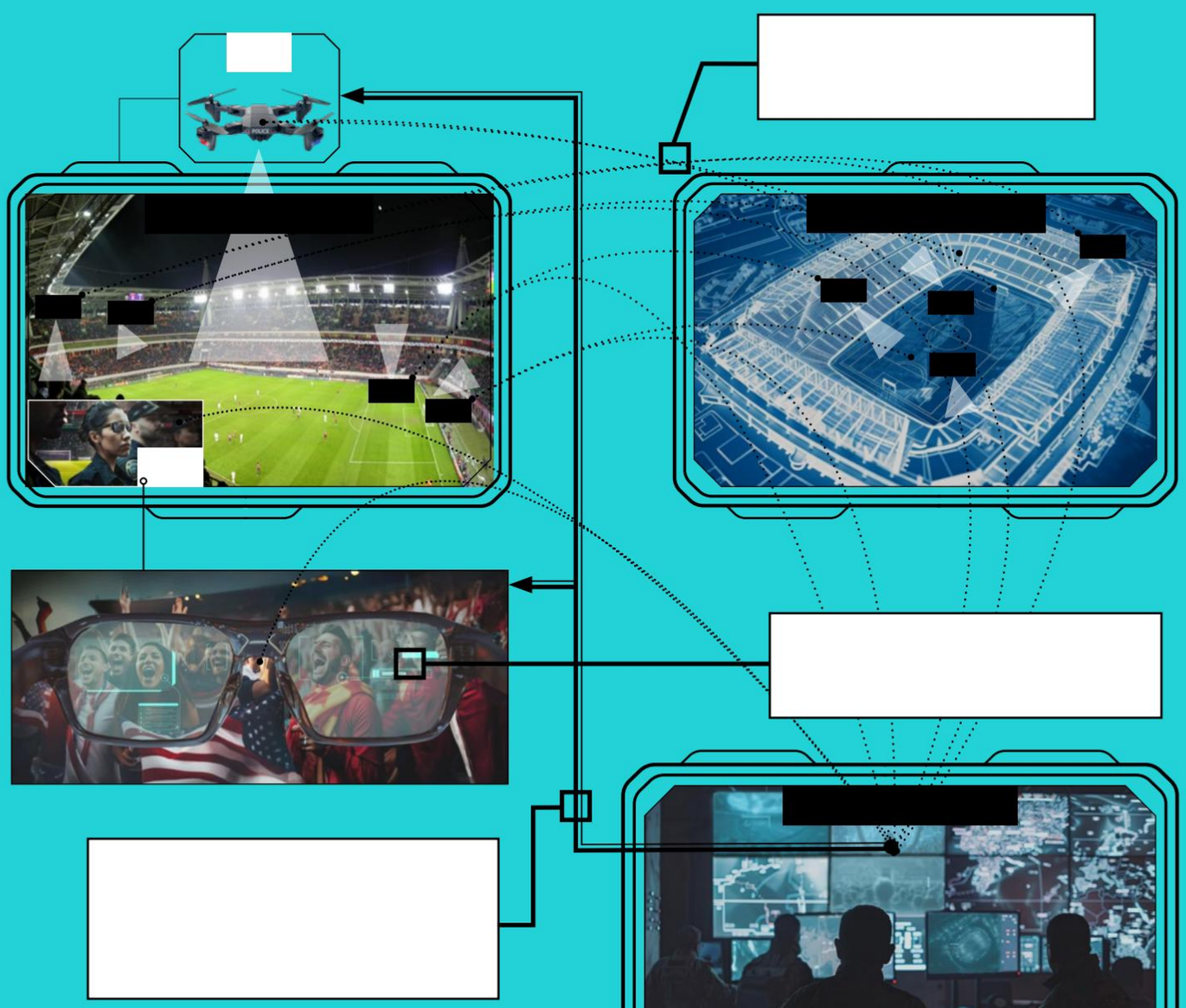


Figure 1 : Les dispositifs portables alimentés par l'IA permettent aux données de circuler de manière transparente entre les agents des forces de l'ordre sur le terrain et le commandement central, ce qui permet à chacun de mieux connaître la situation.

Machine Translated by Google

Imaginez la situation suivante : des milliers de spectateurs affluent vers un stade et une enfant est séparée de ses parents. Ces derniers contactent un agent des forces de l'ordre situé à proximité pour demander de l'aide, mais ils ne parlent pas anglais. Les lunettes connectées de l'agent assurent une traduction instantanée et lui transmettent les détails de la situation par radio. Un autre agent des forces de l'ordre utilise un drone et localise un enfant isolé à 60 mètres de l'endroit où se trouvent les parents. La position de l'enfant est projetée spatialement sur les lunettes de l'agent des forces de l'ordre, qui guide ensuite les parents à travers la foule jusqu'à l'endroit où l'enfant est bloqué.

De l'autre côté du stade, un agent des forces de l'ordre solitaire signale une bagarre entre spectateurs ivres, une bagarre trop importante pour être maîtrisée par une seule personne. Aussitôt, l'officier responsable du poste de commandement affiche un jumeau numérique du stade sur un écran. L'affichage reflète en temps réel la position de chaque agent des forces de l'ordre sur le terrain, chacun équipé d'un équipement technologique permettant une telle précision.

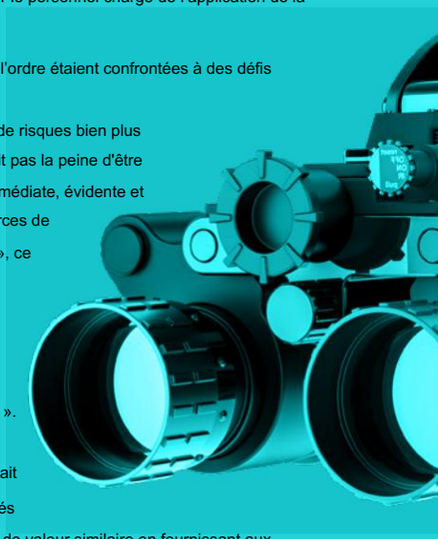
L'officier responsable déploie ensuite un nombre suffisant de personnes pour contribuer à la désescalade de la situation, tout en envoyant d'autres couvrir de nouvelles zones. La localisation et la distance des personnes se présentant pour apporter leur aide sont désormais affichées sur l'écran de l'officier chargé du signalement, guidant ainsi son plan d'intervention.

Dans chacun de ces scénarios, la valeur intrinsèque des dispositifs portables réside dans leur capacité à fournir aux forces de l'ordre travaillant dans des environnements complexes un accès aux données d'une manière et à une vitesse décisives pour répondre aux besoins d'intervention urgents et réguliers. Les technologies qui alimentent ces dispositifs évoluent plus rapidement que jamais.

Sur le marché commercial, de nombreux observateurs se demandent ouvertement si les lunettes à intelligence artificielle remplaceront à l'avenir les écouteurs, voire les téléphones portables. La prochaine étape pour cette technologie consiste à trouver des moyens d'affiner ses capacités afin d'aider le personnel chargé du maintien de l'ordre et de la sécurité publique à accomplir ses missions.

Apprendre des appareils de vision nocturne

Les dispositifs de vision nocturne (NVD) illustrent une technologie portable qui peut créer des avancées révolutionnaires pour le personnel chargé de l'application de la loi.



Avant l'adoption des NVD, les forces de l'ordre étaient confrontées à des défis importants lorsqu'elles opéraient la nuit. Le manque de visibilité s'accompagnait de risques bien plus élevés. Cet équipement lourd ne vaudrait pas la peine d'être emporté sur le terrain sans son utilité immédiate, évidente et indéniable : sa capacité à donner aux forces de l'ordre la capacité de « voir dans le noir », ce qui constitue un avantage considérable.

En d'autres termes, les NVD permettent la « domination des données ». Ils permettent aux forces de l'ordre opérant dans l'obscurité de voir ce qui était auparavant invisible. Les objets connectés alimentés par l'IA offrent une proposition de valeur similaire en fournissant aux forces de l'ordre un accès à des flux de données intuitifs qui améliorent leurs capacités sans augmenter leur charge cognitive.

Carl Ghattas dirige les activités de Booz Allen en matière d'application de la loi et de sécurité intérieure.

Todd Kline est un leader en stratégie et en transformation au sein du marché de l'application de la loi et de l'immigration de Booz Allen, et professeur adjoint à l'Université Bethel.

Thong Nguyen est un technologue centré sur l'humain dans l'incubateur BrightLabs de Booz Allen, axé sur l'avancement une technologie émergente qui transformera les missions futures.

LECTURE RAPIDE

Les technologies portables avancées, notamment les lunettes intelligentes alimentées par l'IA, pourraient fournir aux agents des forces de l'ordre des capacités surhumaines telles que la traduction en temps réel, la détection des menaces et une meilleure connaissance de la situation.

Les forces de l'ordre sont confrontées à un volume écrasant de données provenant de diverses sources, et l'IA pourrait aider à transformer ce « tsunami de données » en renseignements exploitables sur le terrain.

Bien que la technologie pour ces dispositifs portables avancés existe, une mise en œuvre réussie nécessitera un développement minutieux avec les commentaires des utilisateurs pour garantir qu'ils améliorent plutôt qu'ils ne pèsent sur les capacités des agents.

Machine Translated by Google

Booz Allen, président-directeur général
Officier Horacio Rozanski et chef
Matt Calderone, directeur financier de la
Bourse de New York (juin 2024)

Machine Translated by Google

Catalyser l'Amérique Pouvoir d'innovation

Horacio Rozanski, président du conseil d'administration, chef de la direction et président

Voici un vieux dicton : « Si tu veux aller vite, vas-y seul. Si vous voulez aller loin, allez-y ensemble. » Le journal national d'aujourd'hui paysage sécuritaire, le plus difficile auquel nous ayons été confrontés En un demi-siècle, il faut à la fois aller loin et vite.

La capacité à accélérer le développement de technologies révolutionnaires permettra de distinguer les nations qui façonnent l'avenir de celles qui se contentent de s'y adapter.

Alors, comment consolider plus rapidement la domination technologique des États-Unis ? Compte tenu de l'ampleur et de la complexité des défis auxquels notre pays est confronté aujourd'hui, maintenir le statu quo est non seulement insuffisant, mais représente également un risque pour la sécurité nationale. Assurer le maintien de notre suprématie technologique exige une transformation fondamentale de la manière dont notre gouvernement collabore avec l'industrie afin de stimuler l'innovation dans des domaines essentiels à l'équilibre mondial des pouvoirs. D'autres nations, en particulier la République populaire de Chine (RPC) — Nous investissons des ressources massives pour améliorer nos capacités technologiques dans ces domaines clés.

Il est crucial que nous réagissions par une approche nationale. Ce n'est qu'en travaillant ensemble de manière innovante que nous pourrons générer la vitesse et l'élan nécessaires pour maintenir notre position de première puissance technologique mondiale.

L'adoption précoce favorise l'accélération

Prenons l'exemple de l'informatique quantique. Nous sommes engagés dans une course mondiale au développement de l'informatique quantique, avec des implications dans tous les domaines, de la sécurité nationale à l'exploration spatiale en passant par la découverte de médicaments. Le vainqueur de cette course sera celui qui passera le plus rapidement de la théorie à la pratique, du laboratoire à l'application concrète. Et les perdants risquent de perdre bien plus que leur fierté nationale. La RPC collecte probablement des données chiffrées, attendant le jour où les ordinateurs quantiques pourront percer les méthodes de chiffrement actuelles et perturber nos systèmes. On ne saurait trop insister sur le risque que la RPC parvienne à percer nos défenses de cybersécurité plus rapidement que nous ne pouvons percer les leurs.

Face à une telle menace, les secteurs privé et public doivent collaborer de manière innovante. Si l'industrie doit continuer à mener le développement des technologies quantiques et autres technologies avancées, le gouvernement américain peut jouer un rôle d'adepte précoce et, ce faisant, accélérer encore les progrès.

Les entreprises technologiques à la pointe de la technologie ne peuvent réussir sans les early adopters. Ce sont des clients prêts à tolérer les bugs et les produits encore inachevés. En guise de récompense, ils peuvent imaginer comment la nouvelle technologie les aidera à anticiper le marché et, grâce à leurs retours, façonner l'orientation de la technologie. Vous souvenez-vous du premier iPhone ?

Révolutionnaire, mais loin d'être parfait. Si tout le monde avait attendu la perfection, nous utiliserions peut-être encore des BlackBerry.

Machine Translated by Google

« Pour rester en tête, [l'Amérique] doit fonctionner à la vitesse du changement, là où les solutions évoluent aussi vite que les défis et les opportunités émergent. »

Le gouvernement, fort de ses missions à grande échelle et de sa vision à long terme, peut jouer un véritable rôle de catalyseur grâce à ce type d'adoption précoce. La volonté et l'engagement de co-développer les exigences et de tester, itérer et faire évoluer les technologies émergentes aident le secteur privé à franchir les premières étapes de la commercialisation, favorisant une accélération que l'augmentation du financement ne peut à elle seule permettre.

Un nouveau modèle public-privé Collaboration

Aujourd'hui, l'écosystème technologique fédéral n'est pas conçu pour soutenir cette adoption itérative et accélérée de nouvelles solutions techniques. Pour que le gouvernement assume pleinement son rôle d'adepte précoce des technologies, il doit d'abord procéder à une multitude de changements – comme une réforme des acquisitions et une responsabilisation accrue quant aux résultats – qui lui permettront d'agir plus rapidement. Les processus actuels sont conçus pour minimiser les risques, privilégient la prudence et évoluent beaucoup trop lentement pour suivre le rythme rapide des cycles technologiques actuels.

L'industrie, quant à elle, doit considérer le gouvernement non seulement comme un important client en fin de cycle, mais aussi comme un banc d'essai potentiel permettant de repousser les limites du possible. Grâce à une adoption précoce, le gouvernement fédéral gagnerait une place à la table des négociations pour définir les priorités et façonner les résultats qui, à terme, préserveront notre sécurité nationale. Les connaissances acquises permettraient également d'orienter la réglementation en amont des problèmes, et non après. Parallèlement, le secteur privé doit également se considérer comme plus que des concurrents, notamment en matière de sécurité nationale. Nous devons plutôt être des co-investisseurs et Des co-créateurs qui travaillent ensemble pour apporter les solutions dont la nation a besoin. Lorsque ces partenariats sont efficaces, tout le monde y gagne : les missions gouvernementales réussissent plus rapidement, l'innovation américaine progresse à toute vitesse et nos intérêts économiques nationaux sont renforcés.

Chez Booz Allen, nous sommes déjà concrets. Grâce à notre travail, nous sommes une entreprise de technologie de pointe axée sur la rapidité d'exécution pour le gouvernement américain.
Au cœur de l'écosystème technologique fédéral, nous entretenons des relations avec tous les acteurs, des startups et hyperscalers de la Silicon Valley au Pentagone, aux CDC et à la NASA. Nous développons nos propres technologies en nous appuyant sur les meilleures offres commerciales afin d'accélérer l'amélioration significative de la manière dont notre gouvernement sert et protège l'Amérique. Et nous apprenons à travailler plus vite, en interne comme en externe. Nous construisons des partenariats de co-création qui sont déjà à la veille de nouvelles avancées. De l'IA à la cybersécurité, en passant par le logiciel, et du Pacifique à l'orbite, jusqu'ici, nous construisons et collaborons avec les meilleurs acteurs de notre pays, au sein du gouvernement et du secteur privé. L'énergie ainsi créée est impressionnante.

Cette approche, qui associe l'industrie à des investissements conjoints et au développement conjoint de solutions, ainsi que la participation du gouvernement en tant qu'acteur précurseur, est un élément clé du plan d'action global visant à maintenir la suprématie technologique américaine. Pour rester à la pointe, nous devons évoluer au rythme du changement, où les solutions évoluent aussi vite que les défis et les opportunités émergent. Pour y parvenir, il ne suffit pas d'innover brillamment ; il faudra que nous unissions tous nos efforts. Ensemble, nous irons loin et vite.

Machine Translated by Google

RÉFÉRENCES

06. Réflexions sur l'IA générative

Alison Nathan, Jenny Grimberg et Ashley Rhodes, « Gen AI : trop de dépenses, trop peu d'avantages ? » Top of Mind 129, 25 juin 2024, https://www.goldmansachs.com/images/migrated/insights/pages/gs-research/gen-ai--trop-de-depenses,-trop-peu-d'avantages-/TOM_AI%202.0_ForRedaction.pdf.

Brandon Vigliarolo, « Une étude révèle la présence de contenus d'abus sexuels sur mineurs dans un ensemble de données d'entraînement d'IA populaire », The A Register, 20 décembre 2023, https://www.theregister.com/2023/12/20/csam_laion_ensemble de données/.

David Vergun, « La DARPA vise à développer des applications d'IA et d'autonomie auxquelles les combattants peuvent faire confiance », DOD News, 27 mars 2024, https://www.defense.gov/News/News-Stories/Article/Article/3722849/darpa-aims-to-develop-ai-autonomy-applications-warfighters-can-trust/« La DARPA vise à développer des applications d'IA et d'autonomie auxquelles les combattants peuvent faire confiance » > États-Unis Ministère de la Défense > Actualités du ministère de la Défense.

Ethan Mollick, « Quelque chose de nouveau : sur « Strawberry » d'OpenAI et le raisonnement », One Useful Thing, 12 septembre 2024, https://www.oneusefulthing.org/p/something-new-on-openais-strawberry.

« Présentation de l'utilisation de l'ordinateur, un nouveau sonnet Claude 3.5 et un haïku Claude 3.5 », Anthropic, mis à jour le 4 novembre 2024, https://www.anthropic.com/news/3-5-models-and-computer-use.

Jamie Sevilla, Tamay Besiroglu, Ben Cottier, Josh You, Edu Roldán, Pablo Villalobos et Ege Erdil, « La mise à l'échelle de l'IA peut-elle se poursuivre jusqu'en 2030 ? », EpochAI, 20 août 2024, https://epoch.ai/blog/la-mise-a-l-echelle-de-lai-peut-elle-continuer-jusqu-en-2030.

Jory Heckman, « Le DoD crée un outil d'IA pour accélérer le processus obsolète de rédaction des contrats », Federal News Network, 9 février 2023, https://federalnewsnetwork.com/contracting/2023/02/dod-builds-ai-tool-to-accelerate-up-obsolète-process-for-contract-writing/.

Peter Grad, « Une astuce incite ChatGPT à divulguer des données privées », Tech Xplore, 1er décembre 2023, https://techxplore.com/news/2023-12-prompts-chatgpt-leak-private.html

Pranab Sahoo, Ayush Kumar Singh, Sriparna Saha, Vinija Jain, Samrat Mondal et Aman Chadha, « Une étude systématique de l'ingénierie rapide dans les grands modèles de langage : techniques et applications », arXiv, 5 février 2024, https://doi.org/10.48550/arXiv.2402.07927.

10. Réaliser une cyberdéfense en temps réel

« Les cybercriminels ne parviennent pas à s'entendre sur les GPT » SC Media, 28 décembre 2023, https://www.scworld.com/native/cybercriminals-cant-agree-on-gpts.

Zilong Lin, Jian Cui, Xiaojing Liao et XiaoFeng Wang, « Malla : démystifier les services malveillants intégrés au modèle de langage de grande taille du monde réel », prépublication arXiv, 19 août 2024, https://arxiv.org/abs/2401.03315.

17. Retirer la terre des systèmes de mise à la terre

« Accélérer la fusion multi-INT pour les missions de renseignement », Booz Allen Hamilton, consulté le 2 décembre 2024, https://www.boozallen.com/insights/intel/accelerating-multi-int-fusion-for-intelligence-missions.html.

« Accélérer la supériorité spatiale grâce aux plateformes de données ouvertes », Booz Allen Hamilton, consulté le 2 décembre 2024, https://www.boozallen.com/markets/space/accelerate-space-superiority-with-open-data-platforms.html.

Adam Stockley, Les avantages du GSaaS pour l'avenir de l'espace, KDC Resource, 10 février 2023, https://www.kdcresource.com/insights-events/les-avantages-du-gsaas-pour-l-avenir-de-l-espace/.

« DevSecOps avancé pour les missions critiques », Booz Allen Hamilton, consulté le 2 décembre 2024, https://www.boozallen.com/expertise/digital-solutions/devsecops/devsecops-critical-mission-infographie.html.

« aiSSEMBLE : IA à l'échelle de l'entreprise » Booz Allen Hamilton, consulté le 2 décembre 2024, https://www.boozallen.com/expertise/analytics/deployez-lintelligence-artificielle-plus-rapidement-avec-aissemble.html.

Programme de normalisation de la défense, approche modulaire des systèmes ouverts (MOSA), Département de la Défense, consulté le 2 décembre 2024, https://www.dsp.dla.mil/Programs/MOSA/.

Stratégie de données du DoD, ministère de la Défense, 30 septembre 2020, https://media.defense.gov/2020/08/10/2002514180/-1/-1/0/dod-data-strategy.pdf.

Eric Hoffman, Simplifier l'intégration des systèmes spatiaux, Booz Allen Hamilton, consulté le 2 décembre 2024, https://www.boozallen.com/insights/space/simplify-space-systems-integration.html.

Jerome Dunn, Ce que signifie réellement « centré sur le réseau » à « centré sur les données » , Booz Allen Hamilton, consulté le 2 décembre 2024, https://www.boozallen.com/insights/defense/defense-leader-perspectives/what-network-centric-to-data-centric-really-means.html.

Josh Perrius, From the Ground Up, Booz Allen Hamilton, consulté le 2 décembre 2024, https://www.boozallen.com/insights/space/de-la-base-vers-le-haut.html.

« Explication des grands modèles de langage », NVIDIA, consulté le 2 décembre 2024, https://www.nvidia.com/en-us/glossary/grands-modèles-de-langage/.

Sandra Erwin, « Le Pentagone adopte le Starshield de SpaceX pour les futures communications militaires par satellite », SpaceNews, 11 juin 2024, https://spacenews.com/pentagon-embracing-spacexs-starshield-for-future-military-satcom/.

Sandra Erwin, « La rupture des satellites : la volonté des militaires de réduire leurs capacités », SpaceNews, 5 juin 2024, https://spacenews.com/the-satellite-breakup-militarys-push-to-go-small/.

« L'industrie des satellites commerciaux poursuit sa croissance historique tout en dominant le secteur spatial mondial — La SIA publie son 27e rapport annuel sur l'état de l'industrie des satellites » , communiqué de presse du 13 juin 2024, https://sia.org/commercial-satellite-industry-continues-historic-growth-dominating-global-space-business-27th-annual-state-of-the-satellite-industry-report/.

Examen de la politique spatiale et stratégie de protection des satellites, Département de la Défense, 20 septembre 2023, https://media.defense.gov/2023/Sep/14/2003301146/-1/-1/0/rapport-complet-pour-publication.pdf.

« Accélérer les informations de renseignement dans tous les domaines », Booz Allen Hamilton, consulté le 2 décembre 2024, https://www.boozallen.com/insights/intel/speeding-intelligence-insights-across-domains.html.

Transformer plus rapidement les systèmes terrestres spatiaux : 3 façons d'ajouter des capacités flexibles et de contrôler les coûts, Booz Allen Hamilton, 2024, https://www.boozallen.com/markets/space/building-secure-adaptable-space-systems.html.

Machine Translated by Google

Force spatiale américaine, « Le CSO parle de la logique de la supériorité spatiale à l'Institut Mitchell », Communiqué de presse, 29 mars 2024, https://www.spaceforce.mil/News/Article-Display/Article/3725237/.

« Zéro confiance, plus de confiance » Booz Allen Hamilton, consulté le 2 décembre 2024, https://www.boozallen.com/expertise/cybersécurité/architecture-zero-trust.html?origref=&vURL=/zéro confiance.

22. La création de sens réinventée

« Le cadre ADAPT+C », Booz Allen Hamilton, consulté le 29 octobre 2024, https://www.boozallen.com/s/solution/the-adapt-c-framework.html.

Brian Katz, Maintenir l'avantage du renseignement : réimaginer et réinventer le renseignement par l'innovation, Centre d'études stratégiques et internationales, 13 janvier 2021, https://www.csis.org/analysis/maintaining-intelligence-edge-reimagining-and-reinventing-intelligence-through-innovation.

Carmen Medina et Rebecca Fisher, « Ce que la crise économique mondiale devrait nous apprendre », Studies in Intelligence 53, n° 3 (septembre 2009) : 11–16, https://www.cia.gov/ressources/csi/etudes-en-intelligence/volume-53-no-3/ce-que-la-crise-economique-mondiale-devrait-nous-apprendre/.

Conseil d'innovation de la défense, Aligner les incitations pour accélérer l'adoption des technologies, consulté le 29 octobre 2024, https://innovation.defense.gov/Portals/63/20240701%20DIB%20Report_Alignement%20des%20incitations%20ÉTUDE%20PUBLIEE.pdf.

Département de la Défense, Résumé de la stratégie conjointe de commandement et de contrôle dans tous les domaines (JADC2), mars 2022, https://media.defense.gov/2022/Mar/17/2002958406/-1/-1/1/résumé-de-la-stratégie-de-commandement-et-de-contrôle-inter-domaines.pdf.

« Permettre l'apprentissage automatique critique pour la mission », Booz Allen Hamilton, consulté le 29 octobre 2024, https://www.boozallen.com/d/insight/thought-leadership/permettre-lapprentissage-machine-critique-pour-les-missions.html.

« ICArUS : Architectures cognitives et neuroscientifiques intégrées pour comprendre la création de sens », Intelligence Advanced Research Projects Activity, consulté le 29 octobre 2024, https://www.iarpa.gov/research-programs/icarus.

Joseph W. Gartin, « Regard vers l'avenir : l'avenir de l'analyse », Études sur le renseignement 63, n° 2 (juin 2019) : 1–6, https://www.cia.gov/resources/csi/static/Future-of-Analysis.pdf.

Conseil national du renseignement, Tendances mondiales : Paradoxe de Progrès, janvier 2017, https://www.dni.gov/files/documents/nic/GT-Full-Report.pdf.

Bureau du directeur du renseignement national, L' initiative AIM : une stratégie pour augmenter le renseignement à l'aide de machines, consulté le 2 décembre 2024, https://www.dni.gov/fichiers/ODNI/documents/AIM-Strategy.pdf.

Bureau du directeur du renseignement national, Termes et définitions d'intérêt pour les professionnels du contre-espionnage du DoD, 2 mai 2011, https://www.dni.gov/files/NCSC/documents/ci/CI_Glossaire.pdf.

« Citations : Russie », The International Churchill Society, consulté le 24 juin 2023, https://winstonchurchill.org/ressources/citations/russie-2/.

William Burns, « Fireside Chat with William Burns: Aspen Security Forum 2023 », interview de Mary Louise Kelly, 20 juillet 2023, publiée par la Central Intelligence Agency, https://www.cia.gov/static/598a62b34629a8120fb16d68e440aa15/Directeur_Burns_Aspen_Security_Forum_Transcription_07202023.pdf.

32. La technologie à pleine vitesse

Horacio Rozanski, « L'IA et tout : un avenir aux possibilités illimitées », Velocity, 2023, https://velocity.boozallen.com/vue/776121111/82-83/.

Rhiannon Williams, « L'IA générative a appris à un chien robot à se déplacer dans un nouvel environnement », MIT Technology Review, 12 novembre 2024, https://www.technologyreview.com/2024/11/12/1106811/generative-ai-taught-a-robot-dog-to-scramble-around-a-new-environment/.

38. En matière d'apprentissage par l'IA, aucune solution universelle ne convient

« Fiche d'information : Le président Biden publie un décret sur une intelligence artificielle sûre, sécurisée et digne de confiance », La Maison Blanche, 30 octobre 2023, https://www.whitehouse.gov/salle-de-briefing/déclarations-communiqués/2023/10/30/fiche-d-information-le-président-biden-publie-un-décret-exécutif-sur-une-intelligence-artificielle-sûre-sécurisée-et-fiable/.

Mauro Cazzaniga, Florence Jaumotte, Longji Li, Giovanni Melina, Augustus J. Panton, Carlo Pizzinelli, Emma J. Rockall et Marina Mendes Tavares, Gen-AI : Intelligence artificielle et avenir du travail, Fonds monétaire international, 14 janvier 2024, https://doi.org/10.5089/9798400262548.006.

Michelle Cao et Rafi Goldberg, « Déconnecté : pourquoi un foyer américain sur cinq n'est-il pas connecté ? », National Telecommunications and Information Administration, 5 octobre 2022, https://www.ntia.gov/blog/2022/switched-why-are-one-five-us-households-not-online.

41. L'ère de l'IA agentique

« Le gouvernement utilise l'IA pour mieux servir le public », AI.gov, consulté le 16 octobre 2024, https://ai.gov/ai-use-cases/.

Sayash Kapoor, Benedikt Stroebl, Zachary S. Siegel, Nitya Nadgir et Arvind Narayanan, « Agents IA qui comptent », arXiv, 2 juillet 2024, https://arxiv.org/pdf/2407.01502.

46. Là où les algorithmes rencontrent la responsabilité

Ali Farzanehfar, Florimond Houssiau et Yves-Alexandre de Montjoye, « Le risque de réidentification reste élevé même dans les ensembles de données de localisation à l'échelle d'un pays », Patterns 2, n° 3 (12 mars 2021) : 100204, https://doi.org/10.1016/j.patter.2021.100204.

Cynthia Dwork et Aaron Roth, « Les fondements algorithmiques » de la confidentialité différentielle », Fondements et tendances en informatique théorique 9, nos. 3–4 (2014) : 211–407, https://dx.doi.org/10.1561/0400000042.

Jeffrey Mervis, « Les États-Unis ont une nouvelle méthode pour masquer les données de recensement au nom de la confidentialité. Quel est l'impact sur l'exactitude ? » Science, 3 mai 2024, https://doi.org/10.1126/science.zbp0e8r.

Français John M. Abowd, Robert Ashmead, Ryan Cumings-Menon, Simson Garfinkel, Micah Heineck, Christine Heiss, Robert Johns, Daniel Kifer, Philip Leclerc, Ashwin Machanavajjhala, Brett Moran, William Sexton, Matthew Spence et Pavel Zhuravlev, « L'algorithme descendant du système d'évitement de la divulgation du recensement de 2020 », Harvard Data Science Review, numéro spécial 2 (2022), https://doi.org/10.1162/99608f92.529e3cb9.

Machine Translated by Google

Joseph Near et David Darais, Lignes directrices pour l'évaluation des garanties de confidentialité différentielles, National Institute of Standards and Technology, 11 décembre 2023, https://csrc.nist.gov/pubs/sp/800/226/ipd.

Lindsey Choo, « Comment deux étudiants ont utilisé les lunettes Ray-Ban Meta pour accéder à des informations personnelles », Forbes, mis à jour le 4 octobre 2024, https://www.forbes.com/sites/lindseychoo/2024/10/04/méta-ray-bans-ai-surveillance-de-la-vie-privée/.

Michelle Faverio, « Principales conclusions sur les Américains et la confidentialité des données », Pew Research Center, 18 octobre 2023, https://www.pewresearch.org/short-reads/2023/10/18/key-findings-about-americans-and-data-privacy/.

Institut national des normes et de la technologie, « Décret exécutif sur l'intelligence artificielle sûre, sécurisée et digne de confiance : confidentialité différentielle », consulté le 2 décembre 2024, https://www.nist.gov/artificial-intelligence/executive-order-safe-secure-and-trustworthy-artificial-intelligence-0.

« Protection de la vie privée », Government Accountability Office des États-Unis, consulté le 2 décembre 2024, https://www.gao.gov/protection-de-la-vie-personnelle.

Skynova, « La collecte de données : le meilleur ami de l'entreprise », consulté le 2 décembre 2024, https://www.skynova.com/blog/petite-entreprise-big-data.

Ordonnance exécutive n° 14110, 88 Fed. Reg. 75191 (30 octobre 2023), https://www.federalregister.gov/documents/2023/11/01/2023-24283/développement-et-utilisation-sûrs-et-fiables-de-l-intelligence-artificielle.

52. Depuis les premières lignes de la cryptographie post-quantique

« Annonce de l'approbation de trois normes fédérales de traitement de l'information (FIPS) pour la cryptographie post-quantique », National Institute of Standards and Technology, mis à jour le 26 août 2024, https://csrc.nist.gov/News/2024/postquantum-cryptography-fips-approved.

Bureau exécutif du Président, Bureau de la gestion et du budget, « Migration vers la cryptographie post-quantique », 18 novembre 2022, https://www.whitehouse.gov/wp-content/uploads/2022/11/M-23-02-M-Memo-on-Migrating-to-Post-Quantum-Cryptography.pdf.

Bureau exécutif du président des États-Unis, Rapport sur la cryptographie post-quantique, Juillet 2024, https://www.whitehouse.gov/wp-content/uploads/2024/07/ref_pqc-report_final_send.pdf.

Jordan Kenyon et JD Dulny, « À l'ère quantique, la cybersécurité est une course contre la montre », Federal News Network, 8 juillet 2022, https://federalnewsnetwork.com/commentaire/2022/07/à-l-ère-quantique-la-cybersécurité-est-une-course-contre-le-verrou/.

Jordan Kenyon et Taylor Brady, « 5 étapes pour mettre en œuvre les nouvelles normes de cryptographie post-quantique », Semaine de l'information, 5 septembre 2024, https://www.informationweek.com/cyber-resilience/5-steps-for-implementing-the-new-post-quantum-cryptography-standards.

Jordan Kenyon et Taylor Brady, « Cybersecurity in the Quantum Risk Era », Booz Allen Hamilton, consulté le 2 décembre 2024, https://www.boozallen.com/insights/ai-research/cybersécurité-à-l'ère-du-risque-quantique.html.

Loi sur la préparation à la cybersécurité de l'informatique quantique, HR 7535, 117e Congrès (2022) (promulguée, https://www.congress.gov/projet de loi/117e-congrès/projet-de-loi-de-la-chambre/7535/texte.

La Maison Blanche, « Mémorandum de sécurité nationale sur la promotion du leadership des États-Unis dans l'informatique quantique » « Tout en atténuant les risques pour les systèmes cryptographiques vulnérables », communiqué de presse, 4 mai 2022, https://www.whitehouse.gov/briefing-room/statements-releases/2022/05/04/mémorandum-de-sécurité-nationale-sur-la-promotion-du-leadership-des-États-Unis-dans-l-informatique-quantique-tout-en-atténuant-les-risques-pour-les-systèmes-cryptographiques-vulnérables/.

62. Systèmes intelligents à la périphérie

Agence des systèmes d'information de défense Cyber, estimations budgétaires pour l'exercice 2025 , Mars 2024, https://comptroller.defense.gov/Portals/45/Documents/defbudget/FY2025/budget_justification/pdfs/01_exploitation_et_maintenance/o_m_vol_1_part_1/disa_cyber_op-5.pdf.

66. Une autre paire d'yeux

Kristine Steen-Tveit et Bjørn Erik Munkvold, « FromCommon « Image opérationnelle vers une compréhension situationnelle commune : une analyse basée sur les perspectives des praticiens », Safety Science 142 (2021, https://doi.org/10.1016/j.ssci.2021.105381.

Stephen Owsinski, « L'intelligence artificielle dans la police réécrit la rédaction des rapports », National Police Association, consulté le 6 novembre 2024, https://nationalpolice.org/main/artificial-intelligence-in-policing-rewrites-report-writing/.

Thomas J. Cowper et Michael E. Buerger. Améliorer notre Vision du monde : la police et la technologie de réalité augmentée. Groupe de travail sur les contrats à terme PFI/FBI, 2023, https://www.ojp.gov/ncjrs/bibliotheque-virtuelle/resumes/ameliorer-notre-vision-de-la-police-mondiale-et-de-la-technologie-de-realite-augmentee.

Tom McKay, « Voici comment les responsables fédéraux de l'application de la loi utilisent réellement l'IA », IT Brew, 13 juin 2024, https://www.itbrew.com/stories/2024/06/13/voici-comment-les-agents-de-l-application-de-la-loi-fédérale-utilisent-actuellement-l-ai.

Victoria De Cardenas, « Le bureau du shérif du comté de Palm Beach investit 1,3 million de dollars dans l'IA pour rationaliser les rapports de police », WPEC CBS 12, 2 août 2024, https://cbs12.com/news/local/palm-beach-co-sheriffs-office-invests-13-million-in-ai-to-streamline-police-reporting.

72. Catalyser le pouvoir d'innovation de l'Amérique

Menaces chinoises dans le Quantum Euh un , Booz Allen Hamilton, décembre 2021, https://www.boozallen.com/expertise/analytics/quantum-computing/cyber-menaces-chinoises-a-l-ere-quantique.html.

O'Neill, Patrick Howell, « Les États-Unis craignent que des pirates informatiques volent des données aujourd'hui afin que les ordinateurs quantiques puissent les déchiffrer dans une décennie », MIT Technology Review, 3 novembre 2021, https://www.technologyreview.com/2021/11/03/1039171/hackers-quantum-computers-us-homeland-security-cryptography/.

Machine Translated by Google

INFORMATIONS SUR L'AUTEUR DE BOOZ ALLEN

Un merci spécial à tous les dirigeants de Booz Allen qui ont contribué à cette collection et ont fourni une expertise technique et missionnaire tout au long du parcours.

Derek Aucoin
aucoin_derek@bah.com

Marissa Beall
beall_marissa@bah.com

Taylor Brady
brady_taylor@bah.com

Todd Burnett
burnett_todd@bah.com

Christopher Castelli
castelli_christopher@bah.com

Ginny Cevasco
cevasco_virginia@bah.com

Josh Conway
conway_joshua@bah.com

Matt Costello
costello_matthew@bah.com

Joël Dillon
dillon_joel@bah.com

Carl Ghattas
ghattas_carl@bah.com

Joe Gillespie
gillespie_joseph@bah.com

Sean Guillory
guillory_sean@bah.com

Jim Hemgen
hemgen_james@bah.com Rita

Ismaylov
ismaylov_rita@bah.com

Jordan Kenyon
kenyon_jordan@bah.com

Todd Kline
kline_todd@bah.com

John Larson
larson_john@bah.com

Cameron Mayer
mayer_cameron@bah.com

Thong Nguyen
nguyen_thong@bah.com

Josh Perrius
perrius_josh@bah.com

Don Polaski
polaski_donald@bah.com

Edward Raff
raff_edward@bah.com

Joe Rohner
rohner_joseph@bah.com

Horacio Rozanski
rozanski_horacio@bah.com

Mike Saxton
saxton_michael@bah.com

Tony Sharp
sharp_canthony@bah.com

Alison Smith
smith_alison@bah.com

Ernest Sohn
sohn_ernest@bah.com

Éric Syphard
syphard_eric@bah.com

Bill Vass
vass_william@bah.com

Max Wragan
wragan_max@bah.com

Randy Yamada
yamada_randy@bah.com

VELOCIT Y, UNE PUBLICATION DE BOOZ ALLEN

DIRECTEUR DE LA TECHNOLOGIE
Bill Vass

BUREAU DU CTO
John Larson
Julie McPherson

ÉDITORIAL
Rédacteur en chef : John Larson
Rédacteur en chef : Kevin Craft
Stratégie éditoriale : Logan Gibson et Danielle Epting
Consultants éditoriaux : Elana Akman, Éditorial Drumbeat ; Emily Primeaux, Éditorial Libellule

RÉDACTEURS COLLABORATEURS
Dawn Dicker, Pat Fitzgerald et Jim McDermott

CONTRIBUTIONS NOTABLES

CONCEPTION
Direction créative : Chris Walker
Direction artistique et conception : Brody Rose et David Everett

MARKETING ET COMMUNICATION
Responsable de la marque et du marketing : Abby Vaughan
Directrice des médias : Jessica Klenk

Pour toute demande de renseignements de la part des médias, veuillez contacter : Amanda Allison : allison_amanda@bah.com

COMMUNICATIONS ET NUMÉRIQUE
Remerciements particuliers aux personnes travaillant dans les domaines du contenu, du numérique, de la création, de la marque, des médias, du droit, du site Web, de l'accessibilité et de la gestion de projet pour leur soutien à ce projet.

À PROPOS DE BOOZ ALLEN

Booz Allen est une société de technologie de pointe qui fournit des résultats rapides pour les priorités les plus critiques de l'Amérique en matière de défense, de sécurité civile et de sécurité nationale. Nous développons des solutions technologiques utilisant l'IA, la cybersécurité et d'autres technologies de pointe pour faire progresser et protéger la nation et ses citoyens. En nous concentrant sur les résultats, nous permettons à nos collaborateurs, à nos clients et à leurs missions de réussir, accélérant ainsi la réalisation de notre mission : Donner aux citoyens les moyens de changer le monde®.

Pour en savoir plus, visitez BoozAllen.com.

Machine Translated by Google

Booz Allen

Velocity, une publication de Booz Allen, étudie les problèmes complexes qui émergent pour les responsables de mission et de technologie en première ligne de l'innovation gouvernementale.

BoozAllen.com/Velocity