Données massives et intelligence artificielle : un levier stratégique pour la sécurité nationale

Sébastien Lassus

Analyste en sécurité internationale à l'Institut d'études de géopolitique appliquée

29 septembre 2025

ISSN : 2739-3283

Comment citer cette publication :

Sébastien Lassus, *Données massives et intelligence artificielle : un levier stratégique pour la sécurité nationale,* Institut d'études de géopolitique appliquée, Paris, 29 septembre 2025.

121 rue du Vieux Pont de Sèvres 92100 Boulogne-Billancourt
Courriel : secretariat@institut-ega.org
Site internet : www.institut-ega.org

Table des matières

Introduction

Face à la complexification du monde contemporain, le secteur de la défense est confronté à des menaces de plus en plus imprévisibles. Dans ce contexte, l'augmentation exponentielle de la quantité de données numériques constitue un défi majeur : comment exploiter ces vastes ensembles d'informations pour détecter efficacement les menaces potentielles ?

Ces ensembles, communément appelés données massives ou big data, se caractérisent par cinq dimensions fondamentales, souvent désignées comme les « 5 V » : le volume, la vélocité, la variété, la véracité et la valeur. Le volume fait référence à la quantité colossale de données générées chaque seconde : selon des estimations récentes, le volume mondial de données numériques créées ou répliquées a été multiplié par plus de trente en une décennie, atteignant 64 zettaoctets en 2020[1]. Les prévisions indiquent que ce volume pourrait dépasser 180 zettaoctets d'ici 2025, soit une croissance annuelle moyenne de 40 % sur cinq ans. our se représenter l'ampleur de ces données, un zettaoctet équivaut à un milliard de téraoctets, nécessitant 640 millions des plus gros disques SSD actuels (100 To chacun) pour stocker les 64 zettaoctets générés en 2020. Pourtant, malgré cette explosion de données, seulement 2 % des données créées en 2020 ont été sauvegardées en 2021. En conséquence, la capacité de stockage mondiale devrait croître annuellement de près de 20 % entre 2020 et 2025 pour répondre à cette demande croissante[2].

La vélocité désigne la rapidité à laquelle les données sont générées, tandis que la variété renvoie aux différents types de données disponibles, structurées, semi-structurées ou non structurées, provenant de multiples sources telles que les capteurs, les réseaux sociaux ou les sites internet. La véracité fait référence à la qualité et à la fiabilité des données : discerner les informations fiables des données erronées est crucial, car une mauvaise qualité peut conduire à de fausses alertes ou à la non-détection de menaces réelles. Enfin, la valeur représente l'utilité des données, qui dépend du contexte et de l'application, et il est essentiel d'extraire efficacement les informations pertinentes. Ces cinq dimensions sont intrinsèquement liées, et leur gestion optimale est indispensable pour la réussite de la détection des menaces par l'IA.

[1] Bourany T. Les 5V du big data. Regards Croises Sur Econ. 2018;23(2):27–31.
[2] Statista Daily Data [Internet]. 2021 [cited 2024 Jul 20]. Infographie: Le Big Bang du Big Data. Available from: https://fr.statista.com/infographie/17800/big-data-evolution-volume-donnees-numeriques-genere-dans-le-monde

Le traitement des données massives, combiné aux avancées de l'intelligence artificielle (IA), constitue une réponse innovante et incontournable. L'IA permet de dépasser les limites des méthodes d'analyse traditionnelles en traitant des volumes de données sans précédent et en identifiant des schémas complexes invisibles à l'œil humain. Ses capacités d'apprentissage automatique et ses techniques d'analyse prédictive offrent des outils puissants pour la détection précoce des menaces, qu'il s'agisse de cyberattaques, d'actions d'ingérence étrangère ou d'attentats terroristes. Pour assurer une détection efficace, les systèmes d'IA doivent être conçus pour analyser et combiner des données issues de sources variées et hétérogènes.

L'intérêt scientifique pour les données massives a également connu une croissance spectaculaire : le nombre de publications sur le sujet est passé de 2 publications en 2012 à plus de 303 en 2022, soit un taux de croissance annuel moyen de 65,21 %. Cette augmentation s'est particulièrement accélérée à partir de 2019, année marquée par la pandémie de SARS-CoV-2. Sur le plan international, certains pays se distinguent par leur production scientifique dans ce domaine : l'Angleterre, la Chine, les États-Unis, l'Inde et la Malaisie sont parmi les plus influents, la Chine étant actuellement le pays ayant publié le plus d'études sur son territoire[3].

Cependant, l'analyse de données massives par l'IA soulève également des questions éthiques et stratégiques. La sécurité des données, la protection de la vie privée et la souveraineté numérique figurent parmi les préoccupations centrales du secteur de la défense. L'intégration de l'IA repose ainsi sur sa capacité à transformer des données brutes en informations exploitables tout en garantissant la conformité à ces exigences.

Cette étude présentera les principaux enjeux liés à l'exploitation des données massives dans le domaine de la défense et montrera comment l'IA peut contribuer à leur analyse. Il présentera également plusieurs études de cas, en mettant en lumière les applications concrètes et les bénéfices pour le secteur de la défense, tout en abordant les limites et enjeux éthiques associés.

[3] Thayyib PV, Mamilla R, Khan M, Fatima H, Asim M, Anwar I, et al. State-of-the-Art of Artificial Intelligence and Big Data Analytics Reviews in Five Different Domains: A Bibliometric Summary. Sustainability. 2023 Jan;15(5):4026.

État des lieux des méthodes d'analyse des données massives par l'IA

Apprentissage automatique

Les algorithmes d'apprentissage automatique permettent l'automatisation de certaines tâches, réduisant ainsi la nécessité d'interventions humaines. Ils présentent de nombreux avantages, notamment leur précision dans le traitement de vastes volumes de données. Ces algorithmes sont utilisés pour détecter, par exemple, des transactions financières frauduleuses ou le financement d'actions terroristes.

La capacité d'apprentissage des modèles s'améliore proportionnellement à leur exposition aux données, renforçant ainsi leur adaptabilité. Toutefois, cette forte dépendance aux données constitue également leur principale faiblesse[4]. Elle peut être exploitée via l'introduction de données empoisonnées[5], réduisant drastiquement la précision de l'algorithme même avec un faible pourcentage de données compromises.

Une autre vulnérabilité réside dans l'utilisation de portes dérobées[6], qui peuvent être discrètement intégrées dans les données d'entraînement ou les modèles pré-entraînés. Ces portes n'affectent pas les opérations normales du modèle, mais peuvent provoquer des déclassements ciblés lorsqu'une entrée spécifique est fournie. Par exemple, une action d'ingérence étrangère pourrait consister à placer une porte dérobée pour empêcher la détection d'achats de matières premières destinées à produire des explosifs.

Enfin, les modèles peuvent être « volés » via des interrogations répétées du système pour extraire leurs paramètres ou reproduire leur structure[7]. À partir de là, des entrées soigneusement conçues peuvent induire les modèles en erreur et générer des prédictions incorrectes.

[4] Xue M, Yuan C, Wu H, Zhang Y, Liu W. Machine Learning Security: Threats, Countermeasures, and Evaluations. IEEE Access. 2020;8:74720–42.
[5] Données intentionnellement corrompues dans le but d'affaiblir ou biaiser un algorithme d'apprentissage automatique.
[6] Une porte dérobée est un accès secret intentionnellement intégré dans un système informatique, permettant à un utilisateur non autorisé d'y accéder ou de le contrôler sans suivre les procédures de sécurité normales. Cette méthode se différencie des données empoisonnées par son champ d'action généralement plus spécifique.
[7] Attaque par inversion de modèle (model inversion attack) [Internet]. [cited 2024 Jul 20]. Available from: https://www.cnil.fr/fr/definition/attaque-par-inversion-de-modele-model-inversion-attack

Apprentissage profond

L'apprentissage profond est une sous-catégorie de l'apprentissage automatique qui utilise des réseaux de neurones profonds pour analyser des données complexes avec une grande précision. L'architecture de ces réseaux s'inspire du cerveau humain et est constituée de plusieurs couches : entrée, cachées et sortie. La couche d'entrée capture l'information initiale, les couches cachées transforment les données de manière non linéaire, et la couche de sortie produit la classification finale (par exemple : normal ou anormal).

L'application de l'apprentissage profond à la détection des menaces fait notamment appel à des réseaux de neurones convolutionnels (RNC), adaptés aux données en grille comme les images, et à des réseaux de neurones récurrents (RNR), adaptés aux données séquentielles où la sortie précédente sert d'entrée pour l'étape suivante[8].

Le traitement du langage naturel (NLP) constitue également une approche innovante, notamment via l'extraction d'entités nommées (EER), qui identifie et classe des entités dans un texte. Le NLP peut être utilisé pour surveiller les discussions en ligne ou pour analyser les sentiments exprimés dans différentes langues.

Cependant, l'apprentissage profond présente des limites. Il nécessite de vastes quantités de données étiquetées pour un entraînement efficace, ce qui peut être problématique dans le domaine de la défense où l'abondance de données est souvent restreinte. Ces modèles sont également vulnérables aux mêmes attaques que l'apprentissage automatique.

Une solution pour compenser la faible quantité de données consiste à utiliser des réseaux antagonistes génératifs (RAGs), composés d'un générateur et d'un discriminateur, permettant de créer des données synthétiques réalistes. Toutefois, cette approche expose au surapprentissage, où la performance diminue sur des données différentes de celles utilisées pour l'entraînement.

Le déploiement de modèles d'apprentissage profond demande par ailleurs une grande puissance de calcul, les rendant énergivores. Une solution explorée par certaines start-ups, comme FinalSpark en Suisse, consiste à utiliser des bioprocesseurs à base de cultures cellulaires de neurones humains[9]. Cette technologie pourrait réduire la consommation énergétique tout en améliorant la performance.

[8] Jahwar AF, Zeebaree SRM. A State of the Art Survey of Machine Learning Algorithms for IoT Security. Asian J Res Comput Sci. 2021 Jun 16;12–34.
[9] FinalSpark. Biocomputing - The next evolutionary leap [Internet]. 2023 [cited 2024 Jul 20]. Available from: https://finalspark.com/biocomputing-the-next-evolutionary-leap/

Enfin, l'interprétation des décisions de ces modèles demeure difficile, les rendant souvent comparables à des « boîtes noires ». Cette limitation soulève des questions éthiques, notamment sur les biais, car les modèles peuvent reproduire ou amplifier les biais présents dans les données d'entraînement.

Principes généraux de l'intégration de l'IA dans la détection des menaces

L'intégration de l'intelligence artificielle dans la détection des menaces au sein d'un État doit suivre une démarche rigoureuse pour s'avérer efficace. Premièrement, la collecte et la centralisation des données provenant de multiples sources doivent être étudiées afin d'identifier les difficultés rencontrées. Ensuite, les algorithmes doivent être entraînés sur les données recueillies. Enfin, une surveillance continue et des mises à jour régulières s'imposent pour maintenir l'efficacité des modèles d'IA face à l'évolution des menaces. Les algorithmes doivent être recalibrés périodiquement avec de nouvelles données, afin de s'adapter aux tactiques émergentes utilisées par les cybercriminels et les adversaires étatiques.

Les menaces environnementales

L'IA peut contribuer à la modélisation de scénarios liés aux tensions climatiques croissantes. Par exemple, l'outil STRATA, développé par le Programme des Nations Unies pour l'environnement (UNEP), constitue un instrument analytique d'aide à la décision reposant sur l'agrégation de données et sur l'IA. Son utilisation permet une modélisation plus précise des crises[10].

Des systèmes de prédiction de pandémies existent également. EPIWATCH, développé à l'UNSW Sydney, fournit des signaux précoces d'épidémies, tandis que FLUCAST prévoit en temps réel la gravité des saisons grippales, permettant aux systèmes de santé de mieux se préparer[11].

[10] Strata [Internet]. [cited 2024 Jul 20]. Strata - Democratising climate security analysis. Available from: https://unepstrata.org/

[11] MacIntyre CR, Lim S, Quigley A. Preventing the next pandemic: Use of artificial intelligence for epidemic monitoring and alerts. Cell Rep Med. 2022 Dec;3(12):100867.

Dans le domaine informatique, l'IA améliore aussi la cybersécurité en détectant et en prévenant les cyberattaques, notamment les attaques par déni de service distribué (DDoS). Des agents intelligents et réseaux neuronaux permettent d'identifier les anomalies et comportements inhabituels signalant des menaces potentielles. Un exemple est DeepLog, un système de détection d'anomalies basé sur l'IA, capable d'identifier des motifs et des déviations dans les journaux systèmes, révélant des menaces pour la sécurité[12].

Un usage à double tranchant

L'avènement des modèles capables de traiter le langage naturel, tels que ChatGPT, a marqué une révolution dans l'usage de l'IA. Les grands modèles de langage (LLM) rendent ces technologies facilement accessibles au grand public, mais cette accessibilité soulève des préoccupations.

En 2023, le MIT a mené une expérience intitulée « Protéger le futur », visant à évaluer les risques associés aux LLM. Des étudiants non-experts ont testé les usages malveillants possibles. En moins d'une heure, les LLM ont fourni : une liste de quatre pathogènes candidats pour causer une pandémie, des explications sur leur production via la génétique inverse, des fournisseurs potentiels ainsi que des protocoles détaillés[13].

Un autre risque concerne le mésusage des expériences de gain de fonction (GdF), qui consistent à modifier génétiquement des virus pour influencer leur virulence ou leur transmissibilité. Ce type de recherche reste controversé : en 2002, l'équipe d'Eckard Wimmer a synthétisé un poliovirus infectieux à partir d'ADNc sans modèle naturel, ce qui a suscité de vifs débats. En 2018, le virus de la vaccine équine a été reconstruit par synthèse chimique, provoquant de nouvelles controverses, car les méthodes utilisées pouvaient être transposées à la variole, pourtant éradiquée. Une IA pourrait, dans un tel contexte, être exploitée pour concevoir un virus « optimal »[14].

[12] Du M, Li F, Zheng G, Srikumar V. DeepLog: Anomaly Detection and Diagnosis from System Logs through Deep Learning. In: Proceedings of the 2017 ACM SIGSAC Conference on Computer and Communications Security. Dallas, Texas, USA: ACM; 2017. p. 1285–98. Available from: https://dl.acm.org/doi/10.1145/3133956.3134015

[13] Soice EH, Rocha R, Cordova K, Specter M, Esvelt KM. Can large language models democratize access to dual-use biotechnology? [Internet]. arXiv; 2023 [cited 2024 Jul 14]. Available from: http://arxiv.org/abs/2306.03809

[14] Chen H, Liu H, Peng X. Reverse genetics in virology: A double edged sword. Biosaf Health. 2022 Oct 1;4(5):303–13.

Ces risques sont pris très au sérieux : en 2024, le Département de la Sécurité intérieure des États-Unis a publié un rapport sur l'intersection entre IA et risques NRBC (nucléaires, radiologiques, biologiques et chimiques). Celui-ci souligne le double usage de l'IA et recommande un meilleur encadrement de ces technologies[15].

Les limites de l'IA

La Revue de défense nationale a publié en 2019 un article évoquant la doctrine du ministère des Armées sur l'usage de l'IA. Le 5 avril, lors d'une intervention à Saclay, l'IA y est décrite comme un domaine d'« opportunités fabuleuses » et une priorité nationale[16].

Cependant, dès 2020, le Center for Security and Emerging Technology (CSET) publiait un rapport avertissant contre un suroptimisme dans l'application de l'IA à la défense[17]. En effet, l'IA n'est pas une solution miracle, et son usage doit rester rationnel afin d'éviter la dispersion des ressources.

Plus récemment, un rapport de Goldman Sachs (2024) mettait en garde contre une possible « bulle » de l'IA générative, estimant que les transformations majeures n'interviendraient que d'ici une dizaine d'années[18]. Ces injonctions contradictoires compliquent la stratégie du secteur de la défense, où la compétition interétatique est permanente.

Une intégration réussie de l'IA dans la détection des menaces suppose donc une collaboration étroite entre chercheurs, institutions de défense et décideurs politiques. Les investissements doivent être accompagnés d'une surveillance rigoureuse des applications afin de garantir la résilience et l'efficacité des systèmes.

[15] DHS. Fact Sheet and Report: DHS Advances Efforts to Reduce the Risks at the Intersection of Artificial Intelligence and Chemical, Biological, Radiological, and Nuclear (CBRN) Threats. 2024 [cited 2024 Jul 14]. Available from: https://www.dhs.gov/publication/fact-sheet-and-report-dhs-advances-efforts-reduce-risks-intersection-artificial

[16] L'intelligence artificielle et ses applications : un défi stratégique pour la France. Revue de défense nationale. 2019 [cited 2024 Jul 13]. Available from: https://www.defnat.com/e-RDN/vue-article-cahier.php?carticle=148&cidcahier=1188

[17] Center for Security and Emerging Technology, Konaev M, Chahal H, Fedasiuk R, Huang T, Rahkovsky I. U.S. Military Investments in Autonomy and AI: Executive Summary. 2020 Oct [cited 2024 Jul 14]. Available from: https://cset.georgetown.edu/publication/u-s-military-investments-in-autonomy-and-ai-executive-summary/

[18] Goldman Sachs. The impact of generative AI: Too much to spend, too little to benefit. 2024. Available from: https://www.goldmansachs.com/intelligence/pages/gs-research/gen-ai-too-much-spend-too-little-benefit/report.pdf

Conclusion

L’analyse des données massives par l’IA représente une avancée majeure dans la détection et la prévention des menaces à l’échelle mondiale. Ses capacités de traitement de volumes colossaux, d’analyse en temps réel et de découverte de schémas complexes surpassent les méthodes traditionnelles de surveillance et de défense.

Cependant, cette puissance technologique s’accompagne de défis significatifs. Les enjeux éthiques liés à la confidentialité et à la sécurité des données, les risques d’usages malveillants et les vulnérabilités propres aux systèmes d’IA imposent la mise en place de cadres réglementaires robustes et de systèmes résilients, afin de protéger les sociétés contre les abus potentiels.

Institut
EGA

ISSN : 2739-3283

Institut d'études de géopolitique appliquée
121 rue du Vieux Pont de Sèvres 92100 Boulogne-Billancourt
Courriel : secretariat@institut-ega.org
Site internet : www.institut-ega.org