

« Intelligence artificielle, souveraineté et puissance : l'Europe à la croisée des données »

*Par le Commandant Désiré PAQUET, stagiaire EMSST année 2025-2026,
Télécom Paris, Master spécialisé Cybersécurité et Cyberdéfense*

• Introduction

« Celui qui deviendra le leader en intelligence artificielle dominera le monde », déclarait Vladimir Poutine en 2017. Neuf ans plus tard, l'IA est devenue un enjeu central de puissance, au cœur d'une compétition technologique, économique et militaire dominée par les États-Unis et la Chine.

Les États-Unis disposent d'un écosystème complet, associant capitaux privés, soutien public, accès massif aux données et acteurs majeurs comme Nvidia¹, OpenAI² ou Palantir³. La Chine, de son côté, combine financements étatiques et intégration verticale pour développer ses propres modèles, infrastructures de calcul et semi-conducteurs.

Dans ce contexte, l'Europe tente de se positionner comme un acteur souverain et stratégique, en revendiquant une approche éthique à travers des initiatives telles que Mistral AI (acteur français de l'IA) et l'Agence ministérielle pour l'intelligence artificielle de défense (AMIAD), tout en s'efforçant de retenir ses talents et de réduire ses dépendances technologiques.

• Retard européen face aux États-Unis et à la Chine

L'Europe dépend fortement des GPU⁴ Nvidia et de leur écosystème logiciel propriétaire CUDA⁵. Des projets comme le processeur européen Rhea de SiPearl⁶, les supercalculateurs ASGARD⁷ (projet du ministère des Armées opéré par

¹ **Nvidia** – Entreprise américaine spécialisée dans la conception de processeurs graphiques (GPU) et de technologies de calcul haute performance.

² **OpenAI** – Organisation américaine de recherche et de développement en intelligence artificielle, connue notamment pour ChatGPT.

³ **Palantir** – Entreprise américaine développant des logiciels d'analyse et d'exploitation de grandes quantités de données.

⁴ **GPU (Graphics Processing Unit)** – Processeur conçu pour effectuer de nombreux calculs en parallèle, utilisé notamment pour l'IA, le calcul scientifique et le traitement graphique.

⁵ **CUDA** – Plateforme logicielle développée par Nvidia permettant d'utiliser ses GPU pour des calculs intensifs.

⁶ **SiPearl** – Entreprise française concevant des microprocesseurs destinés aux supercalculateurs européens.

⁷ **ASGARD** – Supercalculateur du ministère des Armées dédié aux applications d'intelligence artificielle de défense.

l'AMIAD) et JUPITER⁸ (financé par l'Union européenne et l'Allemagne) renforcent progressivement les capacités européennes de calcul. Toutefois, ils ne suppriment pas la dépendance aux technologies étrangères, et l'Europe reste vulnérable aux ruptures d'approvisionnement et aux restrictions étrangères (contrôles à l'exportation, équipements de fabrication de semi-conducteurs, licences logicielles).

Outre les aspects technologiques, la performance d'un système d'IA dépend aussi de la qualité, du volume, de l'intégrité et de la diversité des données utilisées pour l'entraîner. Sans jeux de données vastes, propres et représentatifs, même les modèles les plus avancés restent limités dans leur précision et leur robustesse.

Le RGPD encadre strictement l'utilisation des données personnelles, tandis que l'AI Act⁹ impose des obligations de conformité et de transparence pour certains systèmes d'IA. Même si les systèmes exclusivement militaires sont exclus de son champ, ces règles peuvent s'appliquer aux usages civils et à certaines technologies dual-use. Elles renforcent la confiance, mais peuvent aussi créer des coûts de conformité et une incertitude juridique. À cela s'ajoute l'absence de consensus entre États membres sur le partage de données sensibles, qui limite la constitution de bases communes à l'échelle européenne.

L'Europe doit donc conjuguer innovation, éthique et sécurité dans un environnement compétitif et fragmenté.

- **Ressources humaines et fuite des talents**

L'Europe dispose d'un vivier de compétences en IA de très haut niveau. De nombreux chercheurs et ingénieurs sont formés et capables de travailler sur des technologies avancées, civiles ou militaires. Pourtant, une part significative des talents européens est attirée par les grands écosystèmes américains et asiatiques, où se concentrent des infrastructures plus puissantes, des financements massifs et des projets industriels d'envergure.

Cette fuite de cerveaux fragilise la souveraineté européenne : sans ces experts, même les infrastructures de calcul européennes et les projets comme Mistral AI ou ceux de l'AMIAD ne peuvent être pleinement exploités.

Pour limiter ce phénomène, l'Europe tente de retenir ou rapatrier les compétences via des programmes d'incubation, des partenariats industrie-université et le développement d'infrastructures souveraines.

⁸ **JUPITER** – Supercalculateur européen installé en Allemagne

⁹ **AI Act** – Règlement européen encadrant le développement et l'utilisation des systèmes d'intelligence artificielle.

Mais le défi reste considérable face à l'attractivité des marchés américains et chinois.

- **L'IA militaire et la guerre des données**

Les conflits actuels illustrent l'usage de l'IA au service de la stratégie militaire.

Drones partiellement autonomes, robots terrestres et algorithmes prédictifs permettent d'améliorer la reconnaissance via l'analyse en temps réel d'images, de naviguer malgré le brouillage du signal GPS et d'accélérer la prise de décision.

Les frappes américaines contre l'Iran en ont donné une illustration récente. Les forces américaines ont eu recours à l'IA pour accélérer l'analyse du renseignement, identifier des cibles potentielles et soutenir la planification des frappes. Selon plusieurs sources, ces opérations auraient notamment reposé sur le Maven Smart System de Palantir, associé à l'IA générative Claude d'Anthropic. Cette séquence constitue l'une des reconnaissances publiques les plus explicites de l'intégration de modèles d'IA commerciaux dans une chaîne de ciblage et de planification militaire.

Parallèlement, la guerre informationnelle est devenue un front stratégique majeur. Deepfakes, campagnes automatisées et publications coordonnées montrent que le contrôle de l'information et de sa diffusion est central dans les opérations contemporaines¹⁰.

En France, VIGINUM a documenté des opérations russes comme Doppelgänger, fondée sur l'imitation de médias, et Portal Kombat/Pravda, réseau de portails diffusant massivement des contenus pro-russes, avec le risque de contaminer l'environnement informationnel exploité par les plateformes et certains modèles de langage.

Ces technologies peuvent reposer sur des logiciels, modèles et chaînes de traitement spécialisés qui, selon leur finalité et leur usage, peuvent relever du régime européen des biens à double usage ou du contrôle français des matériels de guerre et assimilés. Face à la désinformation assistée par IA, les États combinent sanctions, attribution publique, coopération avec les plateformes et obligations de transparence.

- **Conclusion**

¹⁰ <https://www.defense.gouv.fr/desinformation/nos-analyses-froid/janvier-juin-2025-six-mois-desinformation-russe-lencontre-france>

L'intelligence artificielle, les données, les semi-conducteurs et datacenters redéfinissent aujourd'hui les rapports de force géopolitiques. Ces systèmes performants restent fragiles et peuvent être victimes de cyberattaques.

La qualité et l'intégrité des données d'entraînement conditionnent directement la fiabilité des modèles. Cette dépendance aux données crée des vulnérabilités critiques.

Les bases d'entraînement deviennent des cibles pour le vol, la corruption ou l'empoisonnement de données, capables de dégrader silencieusement les performances de l'IA ou d'altérer ses décisions. Que se passerait-il si nos outils d'aide à la décision étaient eux-mêmes corrompus ?

Face à la domination américaine et chinoise, l'Europe, bien que porteuse d'initiatives prometteuses comme Mistral AI ou les supercalculateurs ASGARD et JUPITER, reste fragilisée par sa dépendance technologique, une réglementation parfois restrictive, et la fuite de ses talents.

Pour devenir un acteur crédible, l'Europe devra non seulement sécuriser ses infrastructures et ses données, mais aussi attirer et retenir ses talents, tout en innovant dans un cadre éthique et compétitif.