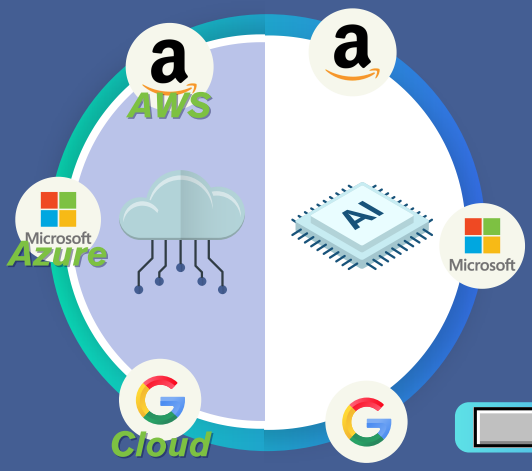
Acteurs du numérique : une place grandissante dans l'industrie de défense

D'abord peu impliquées dans le militaire, les entreprises du numériques s'y intéressent de plus en plus en raison des coûts du développement de l'IA et des contrats de défense lucratifs. Les GAFAM et autres entreprises du numérique s'imposent comme acteurs majeurs de la défense aux États-Unis, via le *Cloud*, l'IA et leurs investissements dans l'industrie de défense.

Gafam = Google, Apple, Meta (Facebook), Amazon, Microsoft

Cloud

Les GAFAM dominent le secteur du ***cloud computing***, en proposant des infrastructures numériques massives. Leurs services cloud sont devenus des piliers technologiques incontournables, notamment pour des applications sensibles dans les domaines stratégiques, gouvernementaux et militaires.



Intelligence artificielle

Les GAFAM occupent une position stratégique dans le développement et la maîtrise des systèmes d'**intelligence artificielle** les plus avancés. Leur expertise technologique en fait des acteurs majeurs de l'IA de défense.

Meta et Apple n'offrent pas de services cloud commerciaux à des clients externes et ne disposent pas des certifications de sécurité exigées pour les contrats défense.

Contrats des GAFAM dans le secteur de la défense

Les GAFAM jouent un rôle central dans le secteur de la défense, à la fois de manière directe et indirecte. Certains contrats sont passés directement avec le Département de la Défense *(DoD)*, tandis que d'autres prennent la forme de partenariats avec des industriels de la défense. Dans les deux cas, les technologies développées, qu'il s'agisse de *cloud computing* ou d'intelligence artificielle sont, *in fine* destinées à des usages militaires.

Parmi les GAFAM, Microsoft est aujourd'hui l'acteur le plus sollicité dans le cadre des contrats de défense gouvernementaux. (FBI, DHS etc.) L'entreprise a développé des versions spécialisées de son cloud : *Azure Government* et *Azure Government Secret*, spécifiquement conçues pour répondre aux besoins sensibles de l'État.

De son côté, Amazon se positionne principalement sur les infrastructures sécurisées via AWS, tandis que Google adopte une approche plus prudente, refusant de s'engager dans des projets impliquant le développement **d'intelligences artificielles létales.**

En 2025, Google a actualisé les principes encadrant le développement de l'intelligence artificielle, en supprimant son engagement à ne pas participer aux armes ou aux systèmes de surveillance.

Parmi les contrats publics

JWCC* *Joint Warfighting Cloud Capability*

JWCC est le *contrat cloud* militaire américain remplaçant JEDI, conçu pour soutenir les opérations militaires via un cloud sécurisé et multi-niveaux. Il sert à héberger, entraîner et déployer des IA de guerre.

- **6** ans 2022-2028
- **9** milliards de dollars
- **4** fournisseurs

(Changement de stratégie car le JEDI ne comprenait qu'un seul fournisseur)

Acteur émergeant : Palantir

Palantir

Créée en 2003 avec le soutien financier de la CIA, la société d'Alex Karp et Peter Thiel fournit au Pentagone un ensemble d'applications militaires dont les apports vont du renseignement jusqu'à la désignation de cible.

Avec la guerre en Ukraine, Palantir a su adapter rapidement ses plateformes (comme Foundry et Gotham) pour intégrer des modules d'IA générative, permettant aux utilisateurs (civils et militaires) de dialoguer avec leurs données, de modéliser des scénarios et de générer des décisions en temps réel.

Palantir s'impose ainsi comme acteur majeur de la défense et décroche de nombreux contrats à l'international.

- **45%** Augmentation des revenus provenant des contrats gouvernementaux
- **3,75** *milliards de dollars* Prévision du chiffre d'affaires 2025
- **64%** Augmentation des revenus provenant des contrats du secteur privé
- **43%** Augmentation des clients de Palantir

Enjeux de souveraineté et géopolitiques

Puissance renforcée des Etats-Unis

Les entreprises du numérique américaines bénéficient d'un soutien étatique et de marchés publics massifs, et sont en position de force pour concurrencer les entreprises européennes.

Avance sur la guerre hybride, cognitive et l'influence.

Souveraineté technologique asymétrique avec le reste du monde, contrôle des flux mondiaux d'informations...

Le modèle américain de collaboration entre l'État et les Big Tech n'a pas d'équivalent en Europe ou en Chine à cette échelle.

Innovation tactique et stratégique beaucoup plus rapide.

La dépendance construite autour des services de Cloud et d'IA réduit drastiquement l'autonomie des autres puissances.

Dépendance de l'Union européenne : quels risques, comment se protéger ?

L'instrumentalisation des données

80%

des technologies numériques-clés de l'Union proviennent de l'extérieur, principalement des Etats-Unis et de la Chine.

70%

Des câbles sous-marins par lesquels transitent les données mondiales sont contrôlés par les GAFAM.

Les entreprises de l'UE ne sont pas autonomes, en cas de conflits ou désaccords avec les Etats-Unis, les données et autres services sont contrôlés à distance et peuvent être un levier de négociations ou d'agression.

RGPD Vs Cloud Act

RGPD : les données des citoyens européens ne peuvent pas être transférées vers des pays ne garantissant pas un niveau de protection équivalent à celui de l'UE.

***Cloud Act* :** il permet aux autorités américaines d'accéder aux données d'individus et d'entreprises (et de leurs clients) situées en dehors des États-Unis à condition que l'entité qui héberge ces données ait un lien avec les Etats-Unis.

Avec le *Cloud Act*, les autorités américaines peuvent désormais demander aux fournisseurs de services américains ou présentant un lien suffisant avec les Etats-Unis de **divulguer les données qu'ils hébergent, même stockées à l'étranger**, à condition que ces données soient associées à un individu ou à une entité relevant de la juridiction américaine.

Extra-territorialité du droit américain

Il est actuellement très difficile pour les entreprises et les éditeurs de logiciels européens d'échapper à l'extraterritorialité du droit américain, à cause de l'omniprésence des GAFAM dans le quotidien personnel et professionnel.

Espionnage industriel

accessibilité facilitée et fuites de données sensibles des concurrents européens pour les États-Unis.

Pression pour atteindre leurs intérêts

La législation extraterritoriale américaine crée un risque d'ingérence via l'accès aux données sensibles des entreprises européennes.

Restriction de marché

Si un produit ou un composant est d'origine américaine ou contient des composants soumis à ITAR, les Etats-Unis peuvent bloquer son exportation vers certains pays.

ITAR

International Traffic in Arms Regulations

L'ITAR impose aux entreprises étrangères de se conformer aux exigences américaines sous peine de lourdes sanctions. Les procédures, complexes et intrusives entraînent des retards de livraison et un risque de perte de contrats, compromettant les réputations à l'international et le développement à l'export des entreprises étrangères.

Quelle stratégie adopte l'OTAN ?

Le 25 mars 2025, l'OTAN a annoncé l'adoption du *Maven Smart System NATO (MSS NATO)*, développé par **Palantir**, pour équiper son Commandement allié Opérations (ACO). Cette plateforme d'intelligence artificielle vise à accélérer la prise de décision sur le champ de bataille.

Un conflit d'intérêts fait surface concernant à la proximité de Peter Thiel, directeur de Palantir, avec le président des Etats-Unis Donald Trump, et de la CIA.

En tant qu'organisation transatlantique, l'OTAN ne favorise pas la souveraineté européenne.

DIANA *(Innovation Defense Accelerator for the North Atlantic)*

Organisme OTAN qui aide des chercheurs et entrepreneurs venant des quatre coins de l'Alliance à développer des technologies destinées à garantir la sécurité des populations des pays de l'OTAN.

NIF *(NATO Innovation Fund)*

Premier fonds de capital-risque multisouverain au monde. Il investira dans des start-up qui développent des technologies de pointe, afin d'exploiter la capacité d'innovation du secteur privé pour répondre aux enjeux de défense et de sécurité critiques.

Comment riposte l'UE ?

Pour que les industriels de défense européens se greffent une place, l'UE et les Etats membres mettent en place plusieurs dispositifs.

RÉSOLUTION EUROPÉENNE *(avril 2024)*
visant à l'application stricte du cadre réglementaire numérique de l'Union européenne et appelant au renforcement des conditions d'une réelle souveraineté numérique européenne.

FED Le Fond Européen de Défense est utilisé pour financer des start-up du numérique, cloud et de l'intelligence artificielle pour renforcer les acteurs de l'UE.

Projet de créer un cloud souverain de l'UE, l'Allemagne et la France conceptualisent **GAIA-X**. Gaia n'est pas un fournisseur de cloud, mais un cadre avec des réglementations qui agit comme organe de certification.

Les industriels européens utilisent des systèmes qui ne sont pas soumis à l'*ITAR* loi qui contrôle les exportations militaires. Parmi eux : Helsing, Thales, Airbus...

FMES Fondation Méditerranéenne d'Études Stratégiques

Sources : Opex news, EUISS, Sénat, Commission européenne