ARCHERY
STRATEGY CONSULTING

INTELLIGENCE ARTIFICIELLE :

Quel modèle collaboratif entre Forces armées et Base Industrielle et Technologique de Défense (BITD) ?

Novembre 2024

A. L'IA REPRESENTE UNE SOURCE D'OPPORTUNITES MAJEURES POUR LA BITD, ET CREE UN CHANGEMENT DE PARADIGME DANS LE SECTEUR DE LA DEFENSE

1. L'IA SE DÉPLOIE À GRANDE ÉCHELLE DANS LA DÉFENSE, PROPULSÉE PAR LE RYTHME DES INNOVATIONS TECHNOLOGIQUES MONDIALES

L'intelligence artificielle est déjà présente sous différentes formes dans la défense, mais son essor actuel marque **une véritable révolution pour la BITD** (9 grands groupes, 4 500 PME/ETI en France).

Passant de l'IA symbolique (basée sur des règles logiques explicites : systèmes d'équations, arbres de décisions, etc.) à des **modèles pouvant être « implicites »** (apprentissage statistique, réseaux neuronaux, etc.) et capables d'apprendre, l'IA permet aujourd'hui à des systèmes d'exécuter des tâches complexes. Grâce au machine learning et au deep learning, alimentés par de vastes ensembles de données annotées, l'IA accomplit des missions comme la reconnaissance d'images (computer vision), l'analyse prédictive et la détection d'anomalies. L'**IA générative** va plus loin en créant du contenu original et en ouvrant des perspectives inédites (conception de systèmes complexes, création d'images satellites synthétiques ou encore planification opérationnelle assistée).

L'essor de l'IA repose sur des **avancées récentes clés** : la puissance de calcul accrue, l'abondance de données (internet, IoT, constellations de satellites), la complexification des algorithmes avancés et la miniaturisation. De plus, l'accessibilité croissante des bibliothèques logicielles et du cloud computing facilite le déploiement de modèles d'IA, sans lourdes infrastructures matérielles et capacités de développement.

Pour les Forces, les applications de l'IA peuvent se décliner en **trois grands domaines : l'IA des opérations, l'IA embarquée et l'IA organique**. Leur objectif est double : accélérer la boucle décisionnelle en temps réel grâce à un traitement optimisé et à l'enrichissement des données, tout en allégeant la charge cognitive des opérateurs, et maximiser l'efficacité opérationnelle, notamment pour la préparation des missions et le MCO.

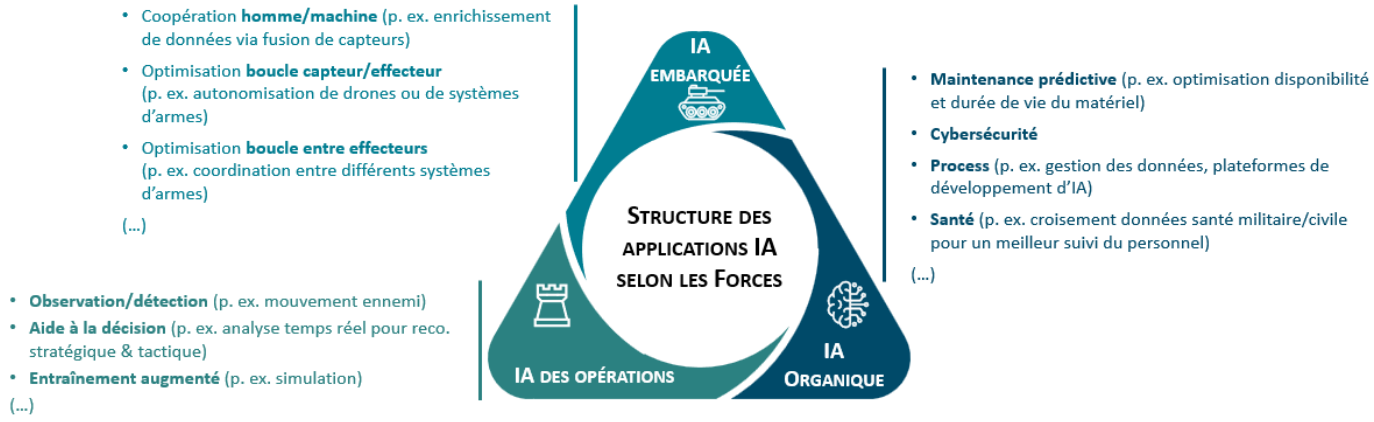

Figure 1 : trois domaines d'application de l'IA pour les Forces

Propulsée par le succès des tests en conditions réelles, l'IA est aujourd'hui de plus en plus intégrée aux écosystèmes de défense, notamment pour l'IA embarquée et l'IA des opérations :

- Les drones ukrainiens utilisés sur le champ de bataille intègrent de l'IA pour la détection d'équipements ennemis grâce à la computer vision, et pour l'automatisation de la navigation, du ciblage et du réajustement de trajectoires (p. ex. drone Saker Scout).
- Aux États-Unis, Shield AI a démontré le potentiel de l'IA dans le domaine du combat aérien, les chasseurs F-16 autonomes ayant systématiquement pris le dessus sur des pilotes humains lors de tests en conditions réelles.
- En France, la DGA a annoncé en 2023 le programme de radar RBE2 XG destiné au Rafale, qui intègrera une IA et une bibliothèque de signaux évolutive destinée à apprendre, à reconnaître et à classer une cible selon sa signature.
- En Europe, l'intégration d'IA dans le SCAF permettra de se coordonner avec des drones autonomes porteurs de charges (brouillage EM, frappes dans la profondeur), eux-mêmes opérés par des modèles d'IA.

Le déploiement de l'IA est confronté à plusieurs enjeux, notamment en Europe : la définition d'un cadre éthique, les biais dus à la discrimination technologique favorisant ou défavorisant certains groupes, l'optimisation des modèles d'IA pour répondre aux exigences de frugalité (en particulier pour l'IA embarquée) ainsi que le développement d'une IA de confiance (valide, robuste, éthique et explicable).

2. L'IA : UN CHANGEMENT DE PARADIGME, IMPACTANT L'ÉCOSYSTÈME DES INDUSTRIELS DE LA DÉFENSE

L'IA agit comme un démultiplicateur d'effets, permettant aux systèmes de traiter davantage d'informations, de gagner en autonomie et en précision. Pendant que le matériel assure la masse et la disponibilité, **la valeur stratégique se déplace de plus en plus vers le logiciel** et la donnée, qui deviennent les moteurs de la performance opérationnelle.

Cette évolution s'accompagne de l'**émergence d'acteurs, qui introduisent des cycles de développement plus courts et des méthodes plus agiles**. Historiquement, l'IA dans la défense était développée en interne par les industriels du secteur, avec des cycles longs et des projets étroitement liés aux besoins militaires. Cependant, cette dynamique a profondément changé, avec le **secteur civil** désormais en tête des avancées technologiques, notamment en matière de calcul, de collecte massive de données et de machine learning. Des initiatives civiles comme OpenAI (ChatGPT) ont démontré le potentiel de l'IA générative, bouleversant l'écosystème technologique et inversant les rôles.

De plus, l'entrée de **nouveaux acteurs**, tels qu'Helsing, Anduril, ou Shield AI, ainsi que des géants technologiques comme Google, Microsoft, ou Palantir (impliqués dans Project Maven, un programme du Pentagone de développement de l'IA pour l'analyse de vidéos de drones), contribue à l'émergence d'une véritable « **DefTech** » (contraction de « Defense Technology »), regroupant les technologies de pointe appliquées à la défense et à la sécurité, telles que l'IA, la cybersécurité ou les drones. Ce phénomène, d'abord observé aux États-Unis, gagne progressivement l'Europe, où un écosystème similaire se développe.

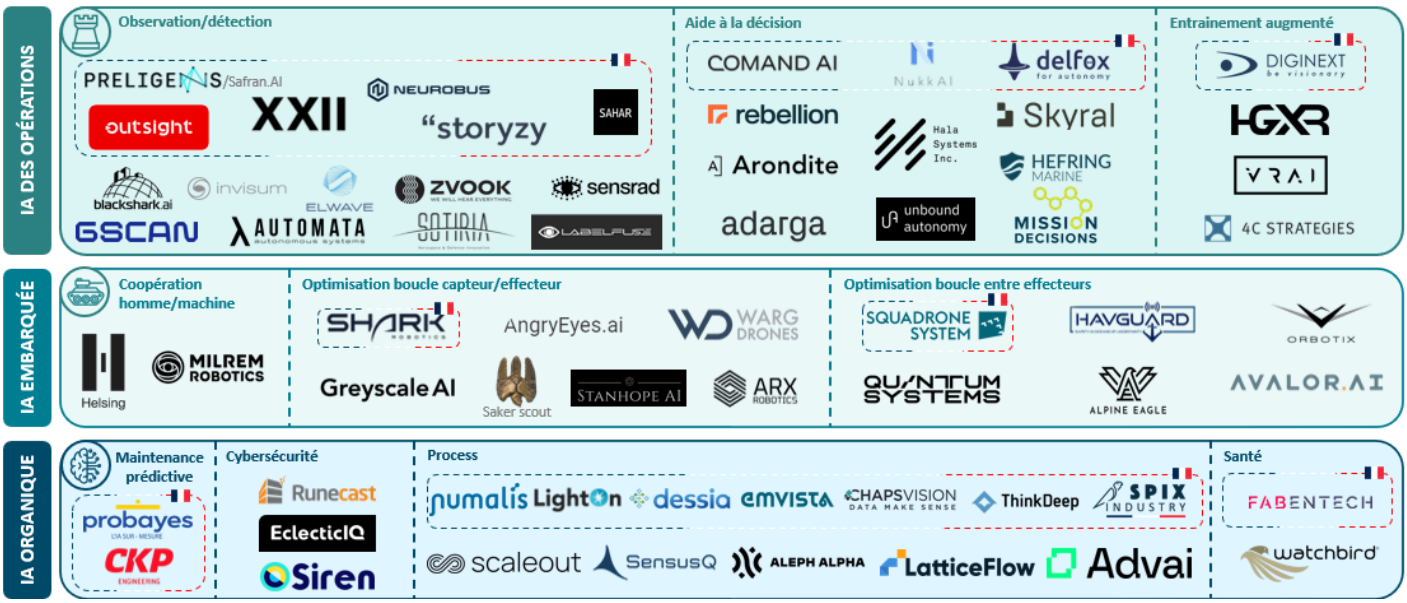

Figure 2 : panorama des start-up/scale-up européennes dans l'IA de défense (DefTech)

Les acteurs historiques de la BITD doivent désormais aligner leurs cycles de développement sur ceux des acteurs agiles, sous peine de les laisser capturer la valeur de l'innovation, a fortiori dans un contexte où les ConOps (« Concepts d'Opérations ») sont encore largement à établir et évoluent rapidement, tout comme les technologies associées. En restant centrés sur le matériel, les industriels risquent de **perdre la maîtrise de la couche intelligente**, essentielle dans la défense moderne. Ceux qui sauront se positionner rapidement sur l'IA auront une opportunité stratégique majeure.

B. FACE AU CHANGEMENT DE PARADIGME IMPOSE PAR L'IA, LA BITD ET LES FORCES DOIVENT RELEVER PLUSIEURS DEFIS

1. AMÉLIORER L'ACCÈS AUX DONNÉES

La performance des modèles d'IA repose avant tout sur leur capacité à apprendre à partir de signaux forts et faibles (aussi appelés « motifs ») contenus dans de vastes quantités de données, autrement dit sur leur « expérience » : plus les données d'entraînement sont riches et diversifiées, plus ces modèles peuvent reconnaître des schémas, prendre des décisions autonomes et s'adapter à des situations complexes. Pour un cas d'usage comme la détection automatique d'objets militaires sur des images satellitaires, cela peut nécessiter plusieurs millions d'images pour entraîner efficacement un modèle. Par ailleurs, les objets d'intérêt évoluent constamment dans le domaine militaire (nouveaux modèles, variantes, camouflages, etc.), rendant crucial l'apport continu de données actualisées.

Cette demande croissante en données est amplifiée par la multiplication des capteurs sophistiqués embarqués sur les plateformes militaires. Par exemple, la surveillance des grands fonds marins (Seabed warfare) génèrerait 1 téraoctet toutes les 1h30, tandis qu'un bataillon porté au standard Scorpion peut produire jusqu'à 30 téraoctets par jour.

Ce **« tsunami » de données** atteint son paroxysme sur un navire de guerre, équipé de nombreux senseurs sophistiqués (radar, sonar, guerre électronique, optroniques, etc.), capturant des données sous-marines, de surface et aériennes. Ce volume massif pose un défi majeur pour les Forces qui manquent de moyens de stockage, de traitement et d'analyse, limitant ainsi l'exploitation efficace de ces informations. La création du Centre de services de la donnée et de l'intelligence artificielle Marine (CSDIA-M) à Toulon témoigne de la prise de conscience par la Marine Nationale de ces enjeux, mais soulève également des questions sur le partage des données.

Le **partage des données** dans le secteur de la défense demeure en effet un enjeu sensible. Les Forces, soucieuses de protéger leurs informations et d'éviter toute fuite, restreignent l'accès aux acteurs externes. Du côté des entreprises de la BITD, bien qu'elles maîtrisent les équipements et puissent générer des données d'entraînement dans des conditions proches du réel (comme Elbit, qui utilise ses propres moyens héliportés pour générer des images à partir de ses optiques), elles hésitent à les partager, les considérant comme un atout concurrentiel clé. Si ces réticences sont en partie légitimes, elles freinent néanmoins les nouveaux acteurs de l'IA, car les données synthétiques ne sont pas suffisantes pour développer des solutions innovantes et accélérer l'intégration de l'intelligence artificielle dans la défense.

Collecter, stocker, trier, annoter, corréler et exploiter : la maîtrise de cette chaîne est indispensable pour garantir non seulement la souveraineté technologique, mais aussi l'efficacité opérationnelle des forces armées face à des menaces en perpétuelle évolution. En réponse à ces enjeux, l'**Amiad** (Agence Ministérielle pour l'IA de Défense) a été créée en mars 2024, avec pour objectif de regrouper 300 spécialistes d'ici 2026 et un budget annuel de 300 millions d'euros : elle centralise données, expertises et infrastructures (notamment un supercalculateur classifié, le plus puissant d'Europe dédié à l'IA). L'agence assurera la gestion souveraine des données, établira des standards pour des collaborations sécurisées et accélérera le développement de solutions IA pour les Forces, renforçant ainsi la souveraineté technologique et clarifiant une doctrine nationale sur l'IA dans la défense.

2. Adapter l'organisation à l'intégration de l'IA et des compétences associées

Face au rythme accéléré de l'innovation, les nouvelles dynamiques de l'écosystème de défense imposent de repenser le **modèle de développement propriétaire de la BITD**. Cependant, certains industriels attachés à leur expertise du domaine hésitent à s'associer à des start-ups de la DefTech, craignant qu'une telle collaboration sans lien capitalistique ne serve de cheval de Troie, abaissant les barrières à l'entrée et favorisant l'émergence de concurrents venus de l'IA, en plus des rivaux industriels traditionnels.

En réponse, de plus en plus d'industriels ont recours à des **partenariats capitalistiques et à des acquisitions** : cela permet d'accélérer l'intégration de nouvelles technologies clés dans l'IA, tout en maitrisant la propriété intellectuelle. Par exemple, Safran a acquis Preligens pour en faire le pilier de sa stratégie IA, et Saab a investi dans Helsing, nouant un partenariat stratégique pour fournir des capacités de guerre électronique basées sur l'IA à l'Eurofighter de la Luftwaffe.

Ce n'est pas la seule approche : d'autres acteurs majeurs de la BITD, comme MBDA et Thales, privilégient la **création de filiales ou d'entités dédiées** (respectivement NEODE Systems et CortAIx), pour accroître leur agilité. Cela permet de concentrer les talents, de mutualiser les connaissances en IA et d'accélérer le développement de solutions innovantes et la diffusion transverse des innovations au sein de ces groupes. En s'affranchissant des processus traditionnels rigides de l'industrie de défense, ces structures favorisent une plus grande réactivité et une capacité à expérimenter plus rapidement avec les technologies émergentes.

La constitution d'un noyau interne (« Make ») en technologies IA ne doit pas être l'unique axe de la stratégie des industriels : l'acquisition (« Buy ») de **briques technologiques civiles** est tout aussi cruciale pour suivre le rythme rapide de l'innovation, avec des solutions établissant les standards de marché (à l'instar des LLM développés par le français Mistral AI). Toutefois, cette approche soulève d'importants enjeux de souveraineté, de cybersécurité et de confidentialité, tout en augmentant la dépendance vis-à-vis des fournisseurs civils : ces solutions sont donc principalement adoptées pour les process et non pour les fonctions critiques.

3. Adopter des modèles de développement logiciels plus ouverts et collaboratifs

Pour répondre à ces enjeux et faciliter l'intégration rapide de technologies civiles, l'adoption d'une **architecture ouverte** apparaît comme une voie privilégiée. Contrairement aux systèmes fermés, ces architectures permettent d'ajouter aisément de nouvelles briques technologiques civiles, telles que l'IA, tout en améliorant l'interopérabilité et en réduisant les coûts et délais. Par exemple, Parrot compense ses limites en R&D grâce à l'une des librairies logicielles open-source les plus actives au monde (kit de développement logiciel ANAFI). Aux États-Unis, le modèle MOSA (Modular Open Systems Approach) garantit flexibilité et interopérabilité, tout en limitant la dépendance aux fournisseurs uniques, encourageant une collaboration plus fluide entre Forces et industriels pour une adoption technologique accélérée.

Adopter une approche agile implique également une redéfinition du rôle des Forces dans le développement des systèmes : plutôt que de suivre un cycle en V rigide, elles doivent passer à une **démarche incrémentale et itérative**, avec des ajustements continus en fonction des retours. Cela exige un suivi renforcé des Forces et des cahiers des charges plus flexibles, capables de s'adapter rapidement aux évolutions technologiques, loin des spécifications figées du modèle traditionnel. Cette démarche itérative permet par ailleurs de réduire le temps nécessaire pour l'intégration des technologies IA dans les opérations de Forces (« Time to market ») afin de pouvoir les tester en conditions réelles.

4. Repenser l'approche du financement et du partage des risques

La montée en puissance du logiciel et des données impose des **investissements massifs** : infrastructure de calcul (serveurs en propre ou cloud computing), acquisition de datasets spécifiques, développement logiciel, etc. Ces efforts sont indispensables pour rester compétitif face à des pays technologiquement en avance comme les États-Unis ou Israël. De plus, l'investissement dans l'IA n'est pas seulement conséquent au départ, il le reste tout au long du cycle de vie des systèmes, en raison des besoins de maintenance et de gestion des évolutions. Ainsi, le modèle de coût évolue progressivement d'un modèle principalement basé sur le CAPEX (dépenses d'investissement) à un **modèle privilégiant davantage l'OPEX** (dépenses opérationnelles). Les industriels doivent donc relever le défi d'innover rapidement, tout en équilibrant des coûts élevés et des risques d'investissements dont la rentabilité pourrait prendre du temps à se concrétiser.

Le financement de ces investissements par l'Etat français reste un défi majeur. Bien que la Loi de Programmation Militaire (LPM) et le plan France 2030 prévoient des budgets significatifs, les **contraintes budgétaires publiques** limitent fortement les marges de manœuvre. Les budgets de défense sont souvent réduits par d'autres priorités nationales, comme la maîtrise du déficit public, et par des **arbitrages budgétaires** internes, même au sein du MinArm (entre programmes comme le PANG, le SNLE 3G, le SCAF ou le RAFALE). Cela exerce une pression constante sur les investissements dans l'innovation, malgré les fonds alloués.

Dans ce contexte budgétaire contraint, les cycles d'acquisition des grands programmes de défense, où l'**innovation planifiée** suit des feuilles de route technologiques précises pour garantir la robustesse et la sécurité des équipements, compliquent l'allocation dynamique des ressources. Il devient difficile d'intégrer l'**innovation ouverte**, souvent impulsée par des start-ups, qui testent des solutions émergentes comme l'IA, encore incertaines ou inconnues au moment d'allouer des financements. Cet équilibre entre innovation planifiée et innovation ouverte, bien qu'il comporte des risques, est pourtant essentiel pour favoriser des avancées industrielles et technologiques majeures.

Face aux difficultés de l'État et des Forces à dégager des budgets pour l'innovation ouverte et à faire émerger des champions dans l'IA, le secteur privé a un rôle crucial à jouer. Historiquement réticents à investir dans les technologies de défense, perçues comme risquées ou à long terme, les **investisseurs privés** commencent à revoir leur position, notamment sur des applications d'IA et de software. Le conflit ukrainien a levé une grande partie des barrières morales à l'investissement dans ce secteur, et la défense est désormais une priorité industrielle pour la Commission européenne. Des opérations comme l'acquisition de Preligens par Safran offrent également des perspectives d'exit plus rassurantes. Cette évolution pourrait encourager un afflux plus important de **capital-risque** vers la DefTech, à l'image des modèles américains avec Anduril ou Shield AI, qui bénéficient de financements conséquents grâce à des partenariats public-privé.

CONCLUSION

L'intelligence artificielle constitue une véritable disruption pour les Forces, tout en présentant des opportunités majeures et un risque de relégation pour les industriels de la BITD. Malgré des initiatives déjà lancées, comme la mobilisation de ressources chez les industriels et la création de l'Amiad par le MinArm, **il manque encore une cohérence d'ensemble** et une maturité dans les modes collaboratifs pour tirer pleinement parti du potentiel de l'IA.

Pour surmonter ces défis, **la BITD et les Forces doivent concentrer leurs efforts sur plusieurs axes stratégiques** : améliorer l'accès aux données, adapter l'organisation à l'intégration de l'IA et des compétences associées, adopter des modèles de développement logiciel plus ouverts et collaboratifs, et repenser l'approche du financement et du partage des risques.

La capacité à s'adapter rapidement déterminera non seulement la compétitivité des acteurs français et européens, mais aussi leur souveraineté technologique à long terme, dans un secteur en pleine transformation.

Guillaume Boutillot
Partner

Antoine Kimmel
Partner

Emmanuel Miremont
Senior Project Manager

CONTACT

ARCHERY STRATEGY CONSULTING
Paris – Toulouse – Tours – Frankfurt – Singapore
www.archeryconsulting.com

Paris Office
14 rue La Boétie
75008 Paris
Tél. +33 (0)1 84 17 02 75

Toulouse Office
9bis Rue de la Colombette
31000 Toulouse
Tél. +33 (0)7 78 41 20 05

Archery Data&Analytics
1 Boulevard Heurteloup
37000 Tours
Tél. +33 (0)6 17 25 01 43

Frankfurt Office
Thurn-und-Taxis-Platz 6
60313 Frankfurt am Main
Tél. +49 (0)151 1965 9269

PVD Singapore
8 Burn Road #08-02/03
Singapore 369977
Tél. +65 9061 1637

ARCHERY
STRATEGY CONSULTING