



L'Europe face au tournant de la *DefTech* Repenser l'écosystème européen d'innovation de défense

Alexandre PAPAEMMANUEL

Laure de ROUCY-ROCHEGONDE

► Points clés

- Aux États-Unis, la *DefTech* prospère du fait d'investissements inédits et d'une financiarisation assumée de l'appareil de défense, permettant de militariser des technologies civiles à grande échelle (spatial commercial, *cloud*, IA).
- Le théâtre ukrainien est un laboratoire de la guerre du futur, où la frontière entre équipements et logiciels s'estompe au profit de systèmes physiques simples mais technologiquement redoutables, renforcés par l'IA, et dont l'usage opérationnel, désormais éprouvé, est voué à s'accroître.
- Émerge alors un nouveau modèle opérationnel fondé sur l'articulation entre « armes de décision » et « armes d'usure », dans un contexte où le numérique conditionne à la fois l'efficacité et la résilience.
- La réponse européenne doit alors être une orchestration de l'hybridation, en rendant compatibles la robustesse des grands groupes industriels et l'agilité des jeunes entreprises, par le biais d'une gouvernance explicite.

Introduction

« La façon dont je vois Iron Dome, c'est l'expression ultime de ce que sera le rôle des États-Unis dans les conflits futurs : non pas être les gendarmes du monde, mais en être l'armurerie¹ », estimait en novembre 2023 Palmer Luckey, le fondateur d'Anduril, l'une des entreprises les plus en vue de la *DefTech*². L'ambition est claire : participer au réarmement mondial en capitalisant sur la qualité des innovations américaines et dominer le marché de l'armement, au moins occidental, par la maîtrise technologique.

Alors que les opérations s'appuient de plus en plus sur la donnée et l'intelligence artificielle (IA) et que les systèmes d'armes deviennent « *software-defined*³ », l'avantage ne se joue plus uniquement dans la conception de plateformes – avions de combat, chars, sous-marins – mais aussi dans la maîtrise de l'architecture informationnelle – collecte, fusion, calcul (*cloud/edge*), interopérabilité – et dans la capacité à innover très rapidement. La guerre, à l'ère de l'IA, ne relève donc pas seulement des États. C'est une affaire à la fois industrielle et logistique, mais aussi financière. Dans cette grammaire post-westphalienne, la souveraineté s'exprime moins en lois qu'en lignes de code. La puissance se mesure en API⁴, en latence de serveurs, en capacité à fusionner capteurs et effets utiles.

Le partenariat industriel noué entre Anduril et Palantir en décembre 2024 est emblématique de cette bascule⁵. Ces deux entreprises dont les patrons viennent de la *tech*, sans ancrage dans la base industrielle et technologique de défense (BITD) américaine, sont aujourd'hui à la pointe des applications de l'IA pour la sécurité nationale, ce qui les place au cœur de la puissance opérationnelle des États-Unis. Cet accord survient au moment où les entreprises technologiques tentent de capter une part plus importante du colossal budget de défense américain – de l'ordre de 900 milliards de dollars pour 2026, et que Donald Trump veut porter à 1 500 milliards de dollars pour 2027 – au détriment des acteurs traditionnels du secteur comme Lockheed Martin, Raytheon ou Boeing⁶. Plus frappant encore, si le consortium Anduril/Palantir est ouvert à « d'autres acteurs du secteur » tels que SpaceX, OpenAI, ou Scale AI, les « *Primes* » n'y sont pas toujours conviés.

1. « Palmer Luckey and Mike Solana on the Future of War, Israel, TikTok Ban, & U.S. Manufacturing », *Pirate Wires Podcast*, 10 novembre 2023, disponible sur : www.youtube.com.

2. La *DefTech* joue, pour la défense, un rôle analogue à celui de la *FinTech* pour la finance et de la *MedTech* pour la santé : elle injecte une logique « produit », logiciel et *data-driven* dans un secteur historiquement dominé par des programmes, des cycles longs et des contraintes réglementaires élevées. Ce terme désigne l'ensemble des entreprises – souvent nées dans l'écosystème startups – qui développent des technologies à usage militaire ou de sécurité (parfois duales), en combinant logiciel, données, IA, capteurs et matériel, avec une logique de produit industrialisable et de déploiement rapide.

3. Est dit « *software-defined* » un système dont le fonctionnement est contrôlé principalement par un logiciel, plutôt que par du matériel fixe.

4. « *Application Programming Interface* » ou interface de programmation d'application.

5. Les entreprises Palantir Technologies et Anduril Industries, spécialisée dans l'analyse de données pour la première et dans les systèmes autonomes pour la seconde, ont lancé début décembre 2024 un consortium afin de répondre aux appels d'offres du Pentagone. Voir le communiqué d'Anduril sur : www.anduril.com.

6. T. Kinder et G. Hammond, « Palantir and Anduril Join Forces with Tech Groups to Bid for Pentagon Contracts », *Financial Times*, 22 décembre 2024, disponible sur : www.ft.com.

L'Europe s'inscrit dans une dynamique comparable, portée par l'essor de jeunes entreprises positionnées sur les segments technologiques les plus avancés⁷. Comme aux États-Unis, la collaboration entre ces nouveaux entrants et les entreprises historiques de la BITD européenne demeure toutefois complexe. Les modalités de l'articulation entre ces deux mondes – innovation agile à partir de la donnée d'un côté, structures établies et centrées sur l'équipement de l'autre – restent largement à définir et les modèles de partenariat, de gouvernance ou d'intégration industrielle sont encore à inventer. Comment, alors, faire converger ces forces pour bâtir une capacité européenne crédible en IA de défense ?

Les leçons de l'Ukraine

Ce basculement de l'ordre industriel accompagne en réalité la rupture stratégique observée sur les théâtres d'opérations contemporains. En effet, en Ukraine comme au Proche-Orient, l'IA n'en finit plus de s'instiller sur le champ de bataille. Ses applications sont aussi nombreuses que protéiformes : de l'observation et la reconnaissance à l'autonomie des systèmes d'armes, en passant par l'identification et la classification des cibles, l'analyse et la prédiction des menaces, la logistique et le ravitaillement, la cybersécurité, la guerre électronique, la simulation et la formation, la santé des armées ou encore l'aide à la décision tactique⁸.

Le conflit russo-ukrainien constitue un laboratoire d'innovation en temps réel, où la distinction conventionnelle entre matériel (*hardware*) et logiciel (*software*) s'efface, redessinant profondément les chaînes de valeur de la défense⁹. La place des drones, souvent produits en masse et à bas coût, atteste de ce revirement : qu'il s'agisse de petits drones à pilotage immersif (FPV), de munitions téléopérées à longue portée ou de drones autonomes, ces systèmes combinent des plateformes physiques simples à des capacités logicielles sophistiquées (IA, guidage autonome, reconnaissance de cible, vision par ordinateur et mise en réseau des signaux) qui maximisent l'effet par rapport au coût¹⁰.

Les Ukrainiens ont ainsi acheté jusqu'à 4,5 millions de FPV en 2025¹¹, pour plus de 2,6 milliards de dollars – une attrition proche d'une économie de la munition. Aux États-

En Ukraine comme au
Proche-Orient, l'IA
n'en finit plus de
s'instiller sur le
champ de bataille

7. C. Boutelet, « À Munich, les start-up du spatial et de la défense dessinent le futur de la tech européenne », *Le Monde*, 16 mai 2025, disponible sur : www.lemonde.fr.

8. A. Férey et L. de Roucy-Rochegonde, « De l'Ukraine à Gaza : l'intelligence artificielle en guerre », *Politique étrangère*, vol. 89, n° 3, Ifri, automne 2024.

9. G. Jones, J. Egan et E. Rosenbach, « Advancing in Adversity: Ukraine's Battlefield Technologies and Lessons for the U.S. », *Policy Brief*, Belfer Center for Science and International Affairs/Harvard Kennedy School, 31 juillet 2023, disponible sur : www.belfercenter.org.

10. K. Bondar, « Ukraine's Future Vision and Current Capabilities for Waging AI-Enabled Autonomous Warfare », Report, Center for Strategic and International Studies/Wadhwani AI Center, mars 2025, disponible sur : www.csis.org.

11. R. Rivaton, « Guerre en Ukraine : l'âge d'or des start-up de la défense », *L'Express*, 29 mars 2025, disponible sur : www.lexpress.fr.

Unis, la montée en puissance des acteurs de la *DefTech* et l'attribution aux géants du numérique (OpenAI, xAI, Google, Anthropic) de contrats de l'ordre de 200 millions de dollars pour le développement opérationnel de techniques d'IA¹² signalent une transition vers une défense pensée comme un système logiciel-industriel, itératif et pouvant être passé à l'échelle.

Dans ce nouveau paysage, le logiciel fait office de ciment stratégique. Il lie le matériel, les capteurs, les flux de renseignement, les plateformes d'observation et les décisions opérationnelles. Le cas du système Delta, déployé par les forces ukrainiennes pour agréger les données issues de drones, de satellites, de radars et d'unités terrestres, en est un exemple probant. En quelques minutes, des frappes peuvent être orientées et des décisions tactiques mises en œuvre, permettant d'accélérer considérablement les boucles de détection, décision et action¹³.

Les acteurs de la *DefTech* financent, conçoivent et déploient leurs innovations sur leurs fonds propres

C'est ce qui fait affirmer à Palmer Luckey que « la technologie est désormais le plus grand avantage sur le champ de bataille¹⁴ » ou à Alex Karp, P.-D.G. de Palantir, que « la seule manière d'éviter la guerre est de posséder la meilleure technologie, et de terroriser l'adversaire¹⁵ ». Si la centralité de la supériorité technologique dans la stratégie américaine n'est pas nouvelle, ces magnats de la *tech* n'attendent plus la permission des institutions pour augmenter l'arsenal militaire.

Contrairement aux grandes firmes tirées par l'expression de besoin des armées qui passent par des appels d'offres et des commandes étatiques, les acteurs de la *DefTech* financent, conçoivent et déploient leurs innovations sur leurs fonds propres (ou levés sur les marchés), avec une vision fondée sur l'anticipation algorithmique, la vitesse de décision et la certitude que les commandes étatiques suivront.

Du capital aux capteurs : un basculement structurel

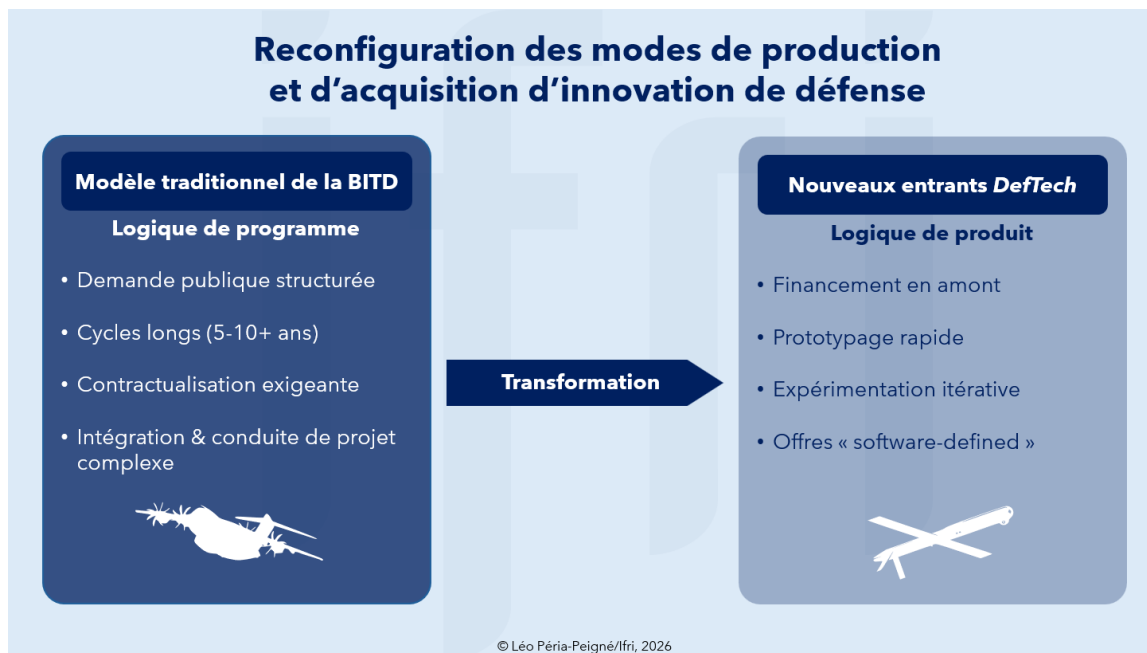
La révolution en cours ne réside pas tant dans l'identité du client, qui demeure l'État, que dans la reconfiguration des modes de production et d'acquisition. Le modèle traditionnel de la BITD repose sur une logique de programme, quand, à l'inverse, les nouveaux entrants de la *DefTech* privilégient une logique de produit.

12. « US Defense Department Awards Contracts to Google, Musk's xAI », Reuters, 14 juillet 2025, disponible sur : www.reuters.com.

13. G. Jones, J. Egan et E. Rosenbach, « Advancing in Adversity: Ukraine's Battlefield Technologies and Lessons for the U.S. », *op. cit.*

14. P. Luckey, « Palmer Luckey: I Saw the Future of War. Now It's up to Us to Prepare for It », *The Free Press*, 8 mai 2025, disponible sur : www.thefp.com.

15. Cité dans M. Dowd, « Alex Karp's Has Money and Power. So What Does He Want? », *The New York Times*, 17 août 2024, disponible sur : www.nytimes.com.



Cette transformation n'implique donc pas un remplacement mais une coexistence durable de deux régimes industriels. Les acteurs historiques conservent un avantage structurel pour l'architecture système, la certification, la souveraineté industrielle, le soutien en service et la gestion des risques. Les nouveaux entrants, quant à eux, appellent à un régime d'innovation plus rapide et concurrentiel, centré sur l'accélération du rythme technologique et la réduction des délais entre conception, test et déploiement capacitaire.

Elon Musk pousse cette logique jusqu'à l'architecture, par le biais d'un écosystème où le réseau devient le centre de gravité stratégique. Starlink fournit ainsi la dorsale de connectivité orbitale utilisée en Ukraine ; tandis que Tesla et, demain, la robotique d'Optimus, apportent des nœuds *edge* massifs *via* l'autonomie ; xAI avec Grok vise la couche d'assistance cognitive et d'exploitation des flux. L'ensemble s'appuie en outre sur une infrastructure énergétique distribuée (Tesla Energy, Powerwall/Megapack) qui renforce la résilience alors que l'électricité, comme la donnée, sont désormais des leviers de coercition. Dans un monde où les infrastructures sont arsenalisées, la puissance tient en effet moins à une plateforme isolée qu'à la capacité d'orchestrer connectivité, calcul embarqué, IA et énergie.

Force est de constater que l'Europe a pour sa part manqué plusieurs rendez-vous dans l'articulation entre innovation technologique et puissance militaire. Contrairement aux États-Unis qui ont su opérer une consolidation industrielle autour du fameux *Last Supper* de 1993¹⁶, à l'origine d'une vague de fusions-acquisitions et d'intégrations verticales qui ont transformé la BITD américaine en un écosystème plus concentré et capable d'absorber des innovations à grande échelle, l'Europe n'a pas su prolonger l'élan

16. N. Hooper, « Another Last Supper and a New Era of Defense Giants », War on the Rocks, 5 mai 2025, disponible sur : <https://warontherocks.com>.

initié avec Airbus, Leonardo et BAE Systems. La tentative de rapprochement EADS–BAE en 2012¹⁷, qui aurait pu créer un champion transnational, a échoué faute d'accord entre États européens sur la gouvernance, les participations publiques et les impératifs de souveraineté et de sécurité, renvoyant l'intégration européenne à des coopérations de programmes et de *joint-ventures* plutôt qu'à une consolidation capitaliste des *Primes*.

Sur le plan opérationnel, elle a souvent été incapable de développer rapidement des applications militaires aux avancées civiles : les mécanismes de transfert, les instruments de financement et les chaînes d'approvisionnement à double usage n'ont pas suffi à capter et à militariser les ruptures technologiques issues du secteur privé. L'Europe n'est pas non plus parvenue à faire émerger et pérenniser des géants du numérique comparables aux acteurs américains ou chinois. L'effort d'industrialisation du logiciel, de l'informatique en nuage et des plateformes de données a été plus timide, avec des conséquences directes sur l'autonomie stratégique et sur la capacité à déployer des solutions souveraines pour la défense.

L'Europe a manqué plusieurs rendez-vous dans l'articulation entre innovation technologique et puissance militaire

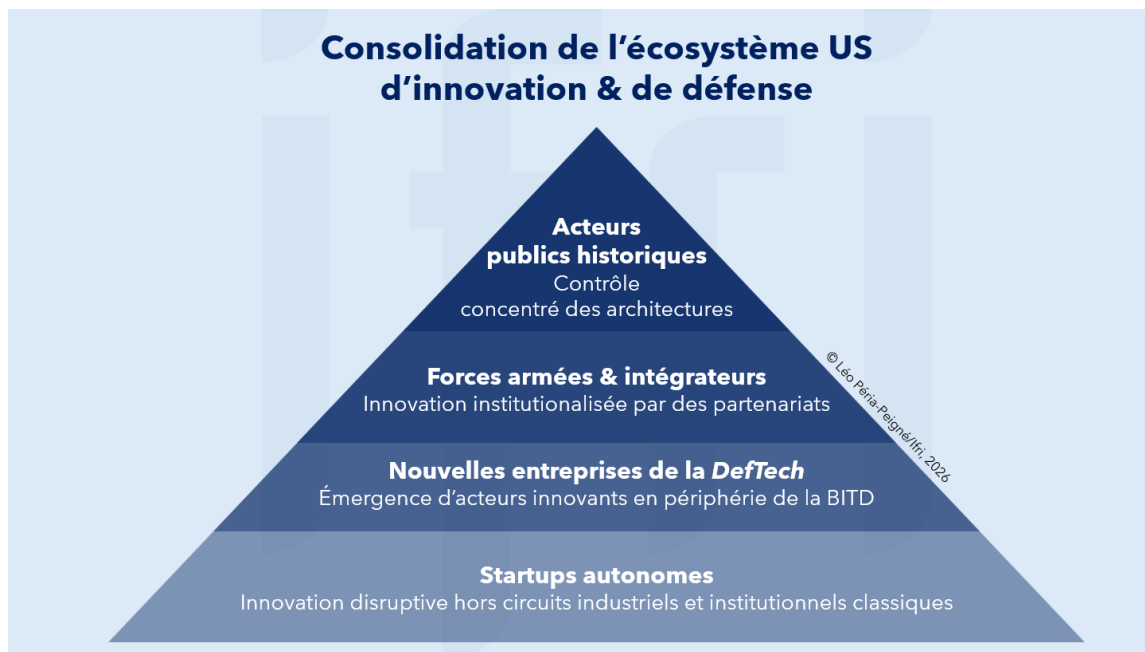
Outre-Atlantique, à l'inverse, la deuxième phase décisive a précisément été celle de la maîtrise de l'infrastructure *cloud*, verrou stratégique pour le stockage et le traitement de données sensibles. Dans le même temps, les données et la connectivité sont devenues des facteurs de puissance à part entière, du fait de la multiplication des capteurs (terrestres, aéroportés, et spatiaux), de la baisse spectaculaire du coût par kilogramme pour accéder à l'orbite terrestre grâce aux lanceurs réutilisables, et de l'émergence d'un renseignement partiellement privatisé – des firmes commerciales s'étant mises à fournir des services de collecte, d'analyse ou d'imagerie pour le secteur de la défense.

La suite logique a été le basculement vers l'*edge computing*, qui permet de traiter et exploiter la donnée au plus près de sa production, directement sur les plateformes et les capteurs, afin de réduire la latence, économiser la bande passante et continuer à opérer même lorsque les liaisons sont dégradées. C'est l'objectif de l'autrefois controversé *Project Maven* du Département de la Défense américain, qui vise à industrialiser l'usage de l'IA pour exploiter des flux de renseignement (notamment l'imagerie et la vidéo produite par les drones), automatiser des tâches jusque-là très consommatrices d'analystes (détection, classification, tri, alertes) et raccourcir la boucle « capteur-décision-effet¹⁸ ». Pendant ce temps, en Europe, l'absence de *Big Tech* et la

17. « Fusion ratée : BAE Systems n'est "plus une option" pour EADS », *Le Monde*, 10 décembre 2012, disponible sur : www.lemonde.fr.

18. Cette démarche de mise à l'échelle pousse progressivement l'inférence et certaines fonctions d'analyse vers l'IA embarquée — et donc vers l'*edge* — afin de rendre le système plus rapide, plus robuste et plus opérationnel. C'est ce qui a permis à des acteurs comme Palantir de capter la valeur en surcouche, une fois l'intégration technique et les fondations de partage, de qualité et de sécurité des données suffisamment stabilisées dans les agences et les armées.

fragmentation des architectures ont laissé ce segment stratégique – plateformes, infrastructures et standards *de facto* – totalement dépendant d'acteurs extra-européens.



La dernière étape a été franchie avec l'entrée massive du capital-risque et des modèles d'intégration produits-plateformes dans un marché historiquement protégé¹⁹. Le *Founders Fund*, dont Peter Thiel a été l'un des principaux argentiers et qui a été le premier investisseur institutionnel dans SpaceX et Palantir, a fait sauter plusieurs verrous juridiques, ouvrant la voie à l'investissement direct dans les technologies d'armement²⁰. Au milieu des années 2010, alors qu'il clôturait son sixième fonds à 1,3 milliard de dollars²¹, le *Founders Fund* s'est en effet distingué par des thèses d'investissement à contre-courant, dont celle de la *DefTech*. Cette inflexion est incarnée en particulier par Trae Stephens — associé du fonds et ancien de Palantir — et par le soutien massif de *Founders Fund* à Anduril, dont il est co-fondateur.

Sous la bannière de l'*American Dynamism*²², conceptualisé début 2022 par Katherine Boyle, associée-fondatrice du fonds de capital-risque a16z, ces investisseurs

19. M. Sion, J. Wenzel et E. Quirk, « Defense Investment at a Turning Point », Bain & Company, septembre 2025, disponible sur : www.bain.com.

20. A. Levy, « Peter Thiel's Founders Fund Closes \$4.6 Billion Growth Fund », The Consumer News and Business Channel, 11 avril 2025, disponible sur : www.cnn.com.

21. S. Martin, « Peter Thiel's Founders Fund Bags \$1.3 Billion », *The Wall Street Journal*, 25 mars 2016, disponible sur : www.wsj.com.

22. L'idée est de rassembler des investissements en faveur d'entreprises dont l'activité sert l'intérêt stratégique des États-Unis — notamment dans l'aérospatial, la défense, la sécurité publique, l'éducation, la construction, la chaîne d'approvisionnement, l'industrie et la fabrication. Depuis la première édition de l'*American Dynamism Summit* début 2023, investisseurs et entreprises se retrouvent à Washington pour renforcer leurs liens avec les responsables politiques. Ce mouvement accompagne le rapprochement croissant entre la Silicon Valley et le pouvoir fédéral, qui marque une nouvelle phase du capitalisme politique américain.

d'un nouveau genre entendent en effet agréger patriotisme et investissements dans la *DefTech*. Josh Wolfe (Lux Capital) fait partie des investisseurs ayant dès 2019 assumé publiquement des paris tournés vers la défense, en soutenant notamment Anduril d'emblée²³. Le fonds de Joe Lonsdale (co-fondateur de Palantir) revendique quant à lui un modèle de *company-building* avec son programme 8VC Build : au-delà de l'investissement, le fonds incube des sociétés (y compris dans la défense, comme dans le cas d'Epirus, fondé en 2018) avant de les faire passer à l'échelle²⁴. Dernier exemple, la structure US *Innovative Technology* de Thomas Tull, apparue fin 2022, mise sur des acteurs à double usage dans le secteur des « technologies critiques d'intérêt national ». Tel est l'ADN des SpaceX, Anduril et d'autres acteurs comme Palantir : la capacité à fusionner matériel, logiciel, et logique de fabrication de défense à très grande échelle.

En Europe, ce type d'acteurs n'a émergé que plus tardivement, et par strates successives. EarthCube, devenu Prelogens, a ouvert la voie du renseignement accéléré par IA avant d'être intégré à un grand groupe industriel en 2024, signe de maturité mais aussi des difficultés à s'émanciper des grands acteurs historiques. Dans une logique complémentaire sur le segment « capteurs », Unseenlabs a fait entrer le spatial commercial dans la chaîne de surveillance, *via* la détection pour la connaissance

maritime. Puis, avec Helsing, Stark et Quantum Systems, une nouvelle génération a émergé en Allemagne à partir de 2020, pour connecter logiciel, autonomie et industrialisation jusqu'à des architectures de reconnaissance-frappe (du drone de renseignement à la munition téléopérée), par le biais de partenariats avec les *Primes*. Plus récemment, en France, des entreprises comme Alta Ares ou Harmattan AI cherchent à porter une ambition plus systémique. Elles entendent transformer le *Command and Control* (C2),

industrialiser l'autonomie et bâtir des capacités dans le segment de l'arme d'usure et de bas de trame, à l'échelle européenne. Tout l'enjeu est alors de leur donner l'espace stratégique et industriel pour croître sans être absorbées.

**Tel est l'ADN des SpaceX,
Anduril et d'autres acteurs
comme Palantir : la capacité à
fusionner matériel, logiciel, et
logique de fabrication de
défense à très grande échelle**

Une querelle des anciens et des modernes ?

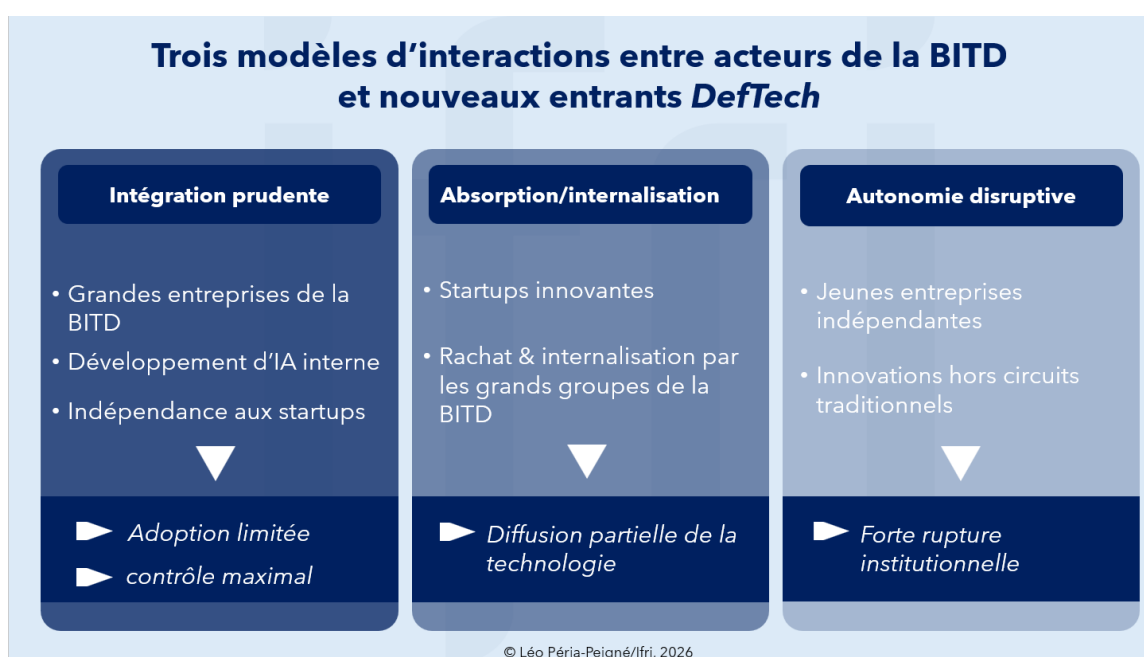
Les industriels historiques s'appuient sur un modèle séquentiel, adossé à des contrats fermes, des jalons normés et des cycles longs. Les nouveaux entrants, eux, cherchent à se passer d'intermédiaires et à interagir directement avec les utilisateurs, selon des

23. J. Wolfe, « A Serious Investment in a Serious Company: Anduril », Lux Capital, 4 octobre 2019, disponible sur : www.luxcapital.com.

24. J. Lonsdale, « Our Duties as Defense Technologists », Joe Lonsdale Blog, 2 novembre 2023, disponible sur : <https://blog.joelonsondale.com>

approches itératives. Ils investissent sans garantie, itèrent vite, misant sur la mise à jour logicielle et la montée en valeur incrémentale.

Jusqu'à présent, l'écosystème de l'IA de défense s'est par conséquent caractérisé par une fragmentation structurelle, résultant du choc entre les acteurs *legacy* de la BITD et ces acteurs émergents. Les premiers, soucieux de préserver leur valeur financière, hésitent à collaborer avec des startups, craignant que ces dernières ne captent une part disproportionnée de la valeur. Parallèlement, ils limitent leur propre prise de risque, n'investissant que lorsque des contrats publics sécurisent l'exploration de nouvelles technologies.



De ce fait, trois modèles d'interaction entre eux se sont fait jour. D'une part, de grands acteurs de la BITD cherchent à incorporer progressivement des capacités d'IA, sans s'appuyer sur des startups, et de manière prudente et limitée²⁵. D'autre part, certains nouveaux entrants, porteurs d'innovations technologiques significatives, se sont vus absorbés ou internalisés par ces mêmes grands groupes, permettant une diffusion partielle de la technologie tout en concentrant le contrôle²⁶. Enfin, une troisième catégorie de jeunes entreprises se développe de manière autonome, en dehors des circuits industriels et institutionnels traditionnels, explorant des solutions disruptives sans être intégrée au cadre classique.

25. MBDA a ainsi créé la structure Neode Système pour accélérer le développement et l'intégration d'IA dans les systèmes du groupe. C'est aussi la démarche de Thales avec cortAIx, ou des dispositifs R&D dédiés chez BAE Systems et Leonardo.

26. Par exemple Safran rachetant Preligens (devenue Safran.AI) ou BAE Systems intégrant BISim (simulation/entraînement).

Les interactions entre « anciens » et « modernes » pâtissent donc d'un manque de confiance mutuelle et de blocages à la fois institutionnels (sécurité, habilitations, conformité), contractuels (propriété intellectuelle, responsabilités, cycles d'acquisition), organisationnels (intégration dans des architectures existantes) et, dans certains cas, réputationnels (acceptabilité politique, médiatique ou interne).

De l'autre côté de l'Atlantique, en revanche, l'opposition entre « anciens » et « modernes » est devenue en partie artificielle. Les grands maîtres d'œuvre disposent de carnets de commandes confortables, tandis que les nouveaux entrants se financent sur des trajectoires d'introduction en Bourse rendues crédibles par des contrats publics déjà significatifs et par l'appétit du capital pour la *DefTech*. Dans ces conditions, le récit d'une « destruction créatrice » où les nouveaux remplaceraient mécaniquement les anciens, résiste mal à l'analyse. La compétition est fortement encadrée par l'État, les coopérations industrielles sont fréquentes, et les frontières entre public et privé sont délibérément entremêlées.

Le véritable point de tension se situe alors en Europe. Faute d'un marché unifié et de capacités de financement et d'industrialisation comparables, les Européens ne disposent ni de la masse critique ni des mécanismes de passage à l'échelle pour soutenir simultanément les industriels établis et de nouveaux entrants souverains. Nombre de startups européennes restent à la peine. Malgré des succès technologiques, elles échouent à franchir les verrous industriels, contractuels et financiers du passage à l'échelle, ce qui freine leur intégration durable dans la BITD et limite, en conséquence, une insertion cohérente de l'IA dans la chaîne de valeur de défense européenne.

En France, la réponse à cette recomposition des affaires capacitaires s'organise autour de trois piliers :

- un pilier souverain, centré sur les programmes les plus critiques et sensibles ;
- un pilier de dépendance croisée, visant des coopérations maîtrisées et réversibles ;
- un pilier marché, fondé sur l'agilité des startups, le capital-risque, les logiques de plateformes et les standards ouverts.

L'État amorce également une inflexion sur la question de l'« arsenalisation » avec la création de l'Agence ministérielle pour l'intelligence artificielle de défense (AMIAD). Néanmoins, en l'absence de gouvernance explicite, de doctrine d'intégration et de financement public structuré, ces initiatives s'exposent à l'échec, à la fragmentation ou à la dilution. L'enjeu n'est donc pas de choisir un modèle unique, mais d'articuler plusieurs régimes d'innovation dans une trajectoire cohérente.

Pour une hybridation stratégique européenne

Les modèles des « anciens » et des « modernes » ne sont en réalité pas incompatibles : ils répondent à des fonctions différentes, de la même manière que les forces spéciales complètent les forces conventionnelles. Se pose en revanche la question de là où réside la principale plus-value militaire – dans les capacités immatérielles ou dans les équipements. Si elle se situe dans l'immatériel, les acteurs historiques deviendront logiquement, à terme, des fournisseurs interchangeables, et les enjeux de souveraineté ainsi que de R&D s'en trouveront relativisés. Cette tension impose alors une synthèse assumée, en permettant des plateformes ouvertes et en imaginant une gouvernance en mesure d'orchestrer des temporalités multiples.

La révolution capacitaire en cours constitue une opportunité historique d'hybridation. À condition de ne pas singer les codes californiens, il est possible de bâtir une alliance pragmatique entre acteurs historiques et nouveaux entrants, où chacun trouve sa place dans une chaîne de valeur repensée. Aux premiers, la sécurité industrielle, l'intégration et l'industrialisation, le passage à l'échelle, les chaînes de qualité maîtrisées ; aux seconds, l'agilité, l'innovation et la vitesse d'adaptation.

Le retour de la guerre de haute intensité impose à l'Europe une double contrainte. D'une part, il est nécessaire d'augmenter significativement les capacités de production pour réarmer l'Europe et reconstruire sa profondeur stratégique. D'autre part, il est indispensable d'intégrer plus rapidement l'innovation technologique au sein des systèmes d'armes et des doctrines de combat. Tandis que les États-Unis ont disposé de près de deux décennies pour transformer leur BITD, l'Europe doit franchir ces étapes dans un laps de temps sensiblement plus réduit, et alors même que Washington se positionne désormais comme le « magasin d'armes » et le fournisseur de l'architecture informationnelle de ses alliés, leur offrant à la fois le matériel, le logiciel et la doctrine.

Face à cette double contrainte, l'Europe n'a d'autre choix que d'articuler deux registres complémentaires : des « armes de décision » (*high-end*) et des « armes d'usure » (*smart and affordable mass*). L'enjeu n'est pas l'arbitrage des deux, mais bien leur combinaison : le *low-end* apporte la masse, sature, fixe et se renouvelle rapidement, tandis que le *high-end* délivre l'effet décisif au moment critique. Cette complémentarité est aussi industrielle : le *high-end* fonde la crédibilité, le *low-end* impose le volume. Il faut à la fois maintenir un portefeuille de plateformes majeures dont la performance est reconnue mais dont la conception demeure peu modulaire et faiblement adaptable, tout en embrassant la révolution en cours.

Il est possible de bâtir
une alliance
pragmatique entre
acteurs historiques et
nouveaux entrants

Cette recomposition doctrinale et industrielle s'appuie sur une nouvelle grammaire capacitaire, qui passe par la massification, la modularité, la logique de « coût cible²⁷ » comme paramètre de conception, la souveraineté technologique, la sécurité fonctionnelle, la robustesse et l'intégration accrue de l'IA comme multiplicateur opérationnel. Sept chantiers doivent être mis en priorité pour y parvenir :

- Diversifier l'écosystème et contractualiser l'hybridation, en évitant de réduire les nouveaux entrants à quelques « champions ». Il est primordial d'organiser un tissu hétérogène, constitué de startups, de PME et d'ETI, y compris à double usage, et de clarifier la chaîne de valeur avec les industriels établis en définissant « qui fait quoi » (briques critiques, intégration système, test et qualification). Pour ce faire, il est possible de mettre en place des clauses type sur l'IP, la responsabilité, la cybersécurité, l'accès au marché, l'export et le partage de revenus pour réduire la défiance et accélérer l'intégration.
- Standardiser des architectures ouvertes « *plug-and-fight* ». Cela passe par la mise en œuvre d'architectures de référence (standards, API, modèle de données, cybersécurité, identités d'accès, exigences de traçabilité), afin de « brancher » des solutions multiples sans verrouillage propriétaire. Sont également souhaitables une certification commune sur les niveaux, les profils et les tests de conformité ; ainsi qu'une gouvernance claire qui fixe le niveau de référence et arbitre les évolutions.
- Accepter des investissements en amont sans exigence contractuelle préalable, en finançant des démonstrateurs et des capacités industrielles avant la commande (prototypage, essais, présérie), afin de réduire le délai entre l'idée et la capacité, et de sécuriser la montée en cadence.
- Faire de la donnée une capacité souveraine mutualisée, en établissant un cadre de « *data commons* » de sécurité (catalogue, niveaux de classification, droits d'usage, anonymisation, traçabilité) pour entraîner et évaluer des modèles, tester l'interopérabilité et accélérer les boucles RETEX.
- Concentrer l'effort sur un petit nombre de « technologies critiques » et piloter par la preuve, pour ne retenir que quelques priorités structurantes (IA appliquée, autonomie, robotique, liaisons, guerre électronique, etc.) et appliquer une discipline de progrès : de courtes *roadmaps*, des revues trimestrielles, des décisions rapides d'arrêt ou de pivot, et des référentiels évolutifs sont à privilégier.
- Muscler le passage à l'échelle, en activant des Capitaux-Risque d'Entreprise européens alignés sur l'enjeu de la souveraineté, et capables de financer non seulement la R&D mais aussi l'industrialisation (chaîne d'approvisionnement) certification, production, export) ; et en prévoyant des trajectoires de sortie compatibles.

27. Le coût-cible n'est alors plus une contrainte traitée à la fin, mais un paramètre de conception dès le départ : l'industriel définit le prix unitaire acceptable (et le coût complet sur le cycle de vie), puis conçoit le système — architecture, matériaux, capteurs, niveau de performance, industrialisation, maintenance — pour respecter ce coût tout en restant militairement pertinent.

- Réduire la friction bureaucratique par le biais de cellules légères dotées d'un mandat clair (décider vite, acheter mieux, intégrer plus vite), avec des processus de test et de qualification accélérés, et une responsabilité explicite sur la livraison de capacités.

Conclusion

Pour la France comme pour l'Europe, l'économie de défense repose désormais sur la coexistence de deux marchés distincts. D'un côté subsistent les systèmes d'armes stratégiques à longue durée de vie, plateformes aériennes, navales ou terrestres, hautement technologiques, coûteuses et pensées pour durer plusieurs décennies. De l'autre émerge un marché nouveau, caractérisé par des capacités consommables, produites en masse, à faible coût unitaire et à cycle d'innovation rapide, dont les drones en Ukraine constituent l'illustration la plus visible. Alors que la guerre de demain s'oriente vers la saturation, l'économie du nombre et la réactivité industrielle, les rapports de force risquent d'être profondément redistribués et les acteurs historiques voient leur leadership contesté. Cette absence d'articulation claire entre les « anciens » et les « modernes » constitue désormais un frein réel : elle fragmente les efforts, ralentit l'innovation et affaiblit la capacité européenne à rester compétitive face aux puissances qui ont déjà opéré ce rapprochement.

Dans ce contexte, l'IA ne saurait être envisagée comme une solution clé en main : elle n'est opérationnelle qu'intégrée dans les chaînes existantes, parfois par incréments modestes, parfois au prix d'une refonte complète des architectures logicielles et décisionnelles. C'est précisément la raison pour laquelle la recherche de démarches européennes adaptées, industrielles, doctrinales et technologiques constitue un enjeu stratégique majeur. Sans capacité à articuler capital technologique et production de masse, l'Europe pourrait se trouver marginalisée dans les conflits de haute intensité à venir. Cela suppose un rôle actif de la puissance publique, non pour arbitrer entre « anciens » et « modernes », mais pour organiser leur hybridation.

Alexandre Papaemmanuel est professeur affilié à Sciences Po Paris et conseiller scientifique Défense de la spécialité Sécurité & Défense de l'École d'Affaires publiques. Ses travaux portent sur le renseignement, la défense et les nouvelles technologies, à l'interface entre analyse stratégique, enjeux opérationnels et politiques publiques. Il est vice-président des Études françaises de Renseignement & Cyber et administrateur de Defense Angels.

Laure de Roucy-Rochegonde est directrice du Centre géopolitique des technologies de l'Ifri depuis février 2024. Ses travaux portent sur les applications militaires de l'intelligence artificielle, la conflictualité normative et la maîtrise des armements. En octobre 2024 est paru son premier ouvrage, intitulé *La Guerre à l'ère de l'Intelligence artificielle : quand les machines prennent les armes* (PUF).

Comment citer cette publication :

Alexandre Papaemmanuel et Laure de Roucy-Rochegonde, « L'Europe face au tournant de la *DefTech*. Repenser l'écosystème européen d'innovation de défense », *Briefings de l'Ifri*, Ifri, 16 février 2026.

ISBN : 979-10-373-1166-5

Les opinions exprimées dans ce texte n'engagent que la responsabilité des auteurs.

© Tous droits réservés, Ifri, 2026

Couverture : © Shutterstock.com



27 rue de la Procession
75740 Paris cedex 15 – France

Ifri.org

