



SEPTEMBRE
2026



Le virage militaire de la *tech* Les algorithmes en ordre de bataille

Benjamin PAJOT

Laure de ROUCY-ROCHEGONDE

L’Ifri est, en France, le principal centre indépendant de recherche, d’information et de débat sur les grandes questions internationales. Créé en 1979 par Thierry de Montbrial, l’Ifri est une fondation reconnue d’utilité publique par décret du 16 novembre 2022. Elle n’est soumise à aucune tutelle administrative, définit librement ses activités et publie régulièrement ses travaux.

L’Ifri associe, au travers de ses études et de ses débats, dans une démarche interdisciplinaire, décideurs politiques et experts à l’échelle internationale.

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

ISBN : 979-10-373-1275-4

© Tous droits réservés, Ifri, 2026

Couverture : Général Randy A. George, chef d’état-major de l’armée de Terre américaine, fait prêter serment à quatre nouveaux lieutenants-colonels lors d’une cérémonie de commissionnement du Detachment 201 : l’Executive Innovation Corps (EIC), à Conmy Hall en Virginie, le 13 juin 2025 [© U.S. Army photo by Leroy Council/DVIDS](#)

Comment citer cette publication :

Benjamin Pajot et Laure de Roucy-Rochegonde, « Le virage militaire de la *tech*.
Les algorithmes en ordre de bataille », *Études de l’Ifri*, Ifri, septembre 2026.

Ifri

27 rue de la Procession 75740 Paris Cedex 15 – FRANCE

Tél. : +33 (0)1 40 61 60 00 – Fax : +33 (0)1 40 61 60 60

E-mail : accueil@ifri.org

Site internet : ifri.org

Auteurs

Benjamin Pajot est chercheur associé au Centre géopolitique des technologies de l'Ifri depuis février 2024 et chercheur indépendant en géopolitique du numérique. Après avoir complété un master d'Histoire contemporaine à l'Enseignement national supérieur de Lyon et un second en Études de guerre à l'Université Paris 1 Panthéon-Sorbonne, il a travaillé comme chargé de mission sur les enjeux numériques et cyber au Centre d'analyse, de prévision et de stratégie du ministère de l'Europe et des Affaires étrangères (CAPS).

Ses recherches portent sur la rivalité technologique sino-américaine, les manipulations de l'information, l'impact sociopolitique des technologies émergentes et les communs numériques. Il s'est également intéressé au suivi du conflit russo-ukrainien dans les domaines cyber et numérique.

Laure de Roucy-Rochegonde est directrice du Centre géopolitique des technologies de l'Ifri depuis février 2024. Elle était précédemment chercheuse au Centre des études de sécurité depuis 2019, où elle a travaillé sur les applications militaires de l'intelligence artificielle, la conflictualité normative et la maîtrise des armements. Docteure en science politique, elle est également chercheuse associée au Centre de recherches internationales (CERI, Sciences Po/CNRS). 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).

Parallèlement à ses activités de recherche, elle enseigne l'éthique de la guerre et la maîtrise des armements à Sciences Po Paris. Elle est par ailleurs titulaire d'un master de politiques publiques et d'une licence de Sciences Po Paris, au cours de laquelle elle a passé une année au département de War Studies du King's College à Londres.

Résumé

Le rapprochement croissant entre les acteurs technologiques et les institutions militaires constitue l'un des bouleversements majeurs de la décennie en matière de conception de la guerre. Après avoir cultivé, dans les années 2010, une image de distance vis-à-vis des usages militaires, dont le retrait de Google du projet Maven en 2018 reste l'épisode le plus emblématique, la Silicon Valley et ses homologues européens embrassent désormais ouvertement les marchés de la défense. Google, Meta, Anthropic, xAI et OpenAI ont décroché d'importants contrats auprès du Pentagone en 2025, tandis qu'en Europe, Mistral AI, Helsing ou Quantum Systems s'inscrivent dans une dynamique comparable.

Cette étude montre cependant que ce virage ne constitue pas une rupture mais un retour aux origines historiques de la Silicon Valley, née des financements militaires de la Seconde Guerre mondiale puis de la guerre froide. Sa nouveauté tient à l'intensité et à la vitesse du phénomène, portées par trois dynamiques convergentes : l'inversion du cycle d'innovation (le civil précède désormais le militaire), l'afflux massif de capitaux publics et de capital-risque vers la défense, et un basculement idéologique qui érige l'engagement militaire des entreprises *tech* en devoir patriotique et en combat contre le *wokisme* supposé de toute une génération de salariés et dirigeants, dans un contexte de retour à des conflits armés de haute intensité.

Des résistances existent, sous la forme de pétitions, démissions et bras de fer entre acteurs privés et puissance publique – à l'image du différend entre Anthropic et le département de la Défense américain –, mais elles demeurent marginales. Les risques induits par cette privatisation rampante de la défense sont pourtant considérables : perte d'expertise étatique et de contrôle des équipements, mais aussi intrusion d'acteurs privés dans la stratégie et la prise de décision militaire. Des risques de dégradation démocratique émergent également, liés à l'utilisation civile de technologies développées à des fins militaires, notamment en matière de surveillance de masse.

Le cas de l'Europe est également abordé dans cette étude, rappelant que l'essor d'un écosystème *DefTech* ne doit pas masquer une dépendance persistante aux infrastructures américaines (*cloud*, puces, modèles fondamentaux). Celles-ci limitent structurellement l'autonomie stratégique européenne et exposent le continent à une vassalisation face aux champions américains.

Executive summary

The growing convergence between technology companies and military institutions is one of the decade's major transformations in the way warfare is conceived. After cultivating an image of distance from military applications throughout the 2010s—with Google's withdrawal from Project Maven in 2018 remaining the most emblematic episode—Silicon Valley and its European counterparts are now openly embracing defense markets. Google, Meta, Anthropic, xAI, and OpenAI secured major contracts with the Pentagon in 2025, while in Europe, Mistral AI, Helsing, and Quantum Systems are following a comparable trajectory.

This study nevertheless shows that this shift does not constitute a rupture, but rather a return to the historical origins of Silicon Valley, which emerged from military funding during the Second World War and the Cold War. Its novelty lies in the intensity and speed of the phenomenon, driven by three converging dynamics: the reversal of the innovation cycle (civilian applications now precede military ones), the massive influx of public funding and venture capital into defense, and an ideological shift that frames the military engagement of tech companies as a patriotic duty and as a struggle against the alleged “wokeness” of an entire generation of employees and executives, against a backdrop of renewed high-intensity armed conflicts.

Resistance does exist, in the form of petitions, resignations, and confrontations between private actors and public authorities, as illustrated by the dispute between Anthropic and the US Department of Defense, but such resistance remains marginal. The risks arising from this creeping privatization of defense are nonetheless considerable: the erosion of state expertise and control over military equipment, as well as the growing involvement of private actors in military strategy and decision-making. Risks of democratic backsliding are also emerging, linked to the civilian use of technologies originally developed for military purposes, particularly in the field of mass surveillance.

The case of Europe is also examined in this study, highlighting the fact that the rise of a European DefTech ecosystem should not obscure the continent's continued dependence on American infrastructure—including cloud services, semiconductors, and foundation models. These dependencies structurally constrain Europe's strategic autonomy and expose the continent to the risk of becoming subordinate to American technology champions.

Sommaire

INTRODUCTION	6
VERS UN COMPLEXE TECHNO-MILITAIRE ?	9
Un retour aux sources.....	9
<i>Des relations historiquement symbiotiques</i>	<i>10</i>
<i>Un phénomène de « revolving doors ».....</i>	<i>12</i>
Un nouveau cycle de l'innovation.....	14
<i>De la tech civilianisée à la tech militarisée.....</i>	<i>15</i>
<i>Un antimilitarisme de façade ?</i>	<i>17</i>
<i>Des technologies duales par nature</i>	<i>18</i>
« WE MUST REBEL AGAINST THE TYRANNY OF THE APPS »	21
Le double tournant de la pandémie et de l'invasion russe de l'Ukraine	21
L'avènement d'un « patriotisme <i>in tech</i> »	22
DE LA DISTANCE AFFICHÉE AU RAPPROCHEMENT ASSUMÉ	26
L'opportunisme mercantile face à une offre étatique exponentielle.....	26
Le capital-risque sous la bannière de l'<i>American Dynamism</i>	29
L'hypothèse d'un « <i>backlash</i> »	32
VERS UNE PRIVATISATION DE LA DÉFENSE ?	34
Un empiètement sur les fonctions régaliennes.....	34
La matrice de bascules autoritaires	36
Des résistances encore modestes	38
UNE EUROPE ENFERMÉE DANS UNE DÉPENDANCE STRUCTURELLE ?.....	40
CONCLUSION	44

Introduction

Le 15 février 2025, dans son discours d'adieu en tant que président des États-Unis, Joe Biden alertait sur l'influence exercée par le « complexe techno-industriel » formé par les oligarques de la *tech*¹. De fait, quelques jours plus tard, tous les patrons des *Big Tech*, d'Amazon à Google en passant par Meta et OpenAI, se serraient au premier rang de la seconde cérémonie d'investiture de Donald Trump².

Cette mise en garde n'est pas sans rappeler celle formulée soixante-quatre ans plus tôt par Dwight Eisenhower, dans sa propre allocution de départ de la Maison-Blanche, sur les dangers du « complexe militaro-industriel³ » :

« Dans les prises de décision de l'État, nous devons donc nous garder de toute influence injustifiée, qu'elle ait ou non été sollicitée, exercée par le complexe militaro-industriel. Le risque potentiel d'une désastreuse ascension d'un pouvoir illégitime existe et persistera. »⁴

En 2025 comme en 1961, ces présidents sortants ont souhaité consacrer leurs derniers mots aux périls que font peser sur la démocratie les abus de pouvoir de quelques-uns. Aujourd'hui, il serait même possible de parler d'un « complexe techno-militaire », tant les liens entre le secteur technologique et les institutions militaires se sont étoffés ces dernières années, témoignant d'une exacerbation de la dualité des technologies⁵.

Il n'en a pas toujours été ainsi. Dans les années 2010, de nombreuses entreprises du numérique – en particulier dans la Silicon Valley – affichaient une réticence à collaborer avec les forces armées. Le cas du projet Maven, dont Google s'était retiré en juin 2018 sous la pression de ses salariés⁶, est emblématique des résistances culturelles qui se manifestaient alors au sein de ce qu'on appelait encore les GAFAM (Google, Apple, Facebook, Amazon, Microsoft) et de l'importance des préoccupations éthiques et

1. La *tech* désigne l'ensemble du secteur des technologies numériques et de l'innovation, incluant les entreprises, les métiers et les outils liés à l'informatique, aux logiciels, à l'intelligence artificielle, aux applications et à Internet. Ce terme est utilisé pour parler à la fois des grandes entreprises technologiques comme Google ou Apple, mais aussi de tout l'écosystème des startups et des innovations numériques qui y voient le jour.

2. S. Baker, « Tech CEOs Flock to Trump's Inauguration », *Axios*, 17 janvier 2025.

3. Discours de fin de mandat de Dwight D. Eisenhower, allocution télévisée, 17 janvier 1961.

4. *Ibid.*

5. R. Bacqué, D. Leloup et A. Piquard, « De l'IA à l'armée, les oligarques de la tech étendent leur empire », *Le Monde*, 25 juillet 2025.

6. Le controversé projet Maven avait initialement pour but d'améliorer l'analyse des images vidéo filmées par les drones de l'armée américaine. Récupéré par Palantir, le contrat a considérablement évolué par la suite, mais nous y reviendrons.

réputationnelles liées à l'usage militaire des technologies. Il y a encore trois ans, certains acteurs de la *DefTech*, tel Castelion, peinaient à ouvrir un compte bancaire dans la Silicon Valley, du fait de la stigmatisation qui pesait sur les activités d'armement et de renseignement⁷.

Alors que dans le champ militaire le logiciel semble prendre le pas sur le matériel, le déclenchement de la guerre en Ukraine à l'hiver 2022 s'est accompagné d'une évolution profonde du rapport entre les grandes firmes technologiques et le secteur de la défense. Des acteurs qui affirmaient autrefois leur distance vis-à-vis des usages militaires opèrent aujourd'hui un virage stratégique. Ce dernier se voit notamment encouragé par la financiarisation galopante des secteurs du numérique et de la défense, sous la houlette d'un capital-risque en quête de nouvelles marges de rentabilité. Il est également renforcé par la frénésie militariste qui caractérise la seconde administration Trump, ouvrant la voie à un alignement d'intérêts aux relents techno-nationalistes, auquel l'Europe répond par des tentatives de rattrapage encore timides.

Au cours de l'année 2025, nombre de *Big Tech* ont ainsi annoncé avoir obtenu de lucratifs contrats auprès du département de la Défense (DoD). Ainsi de Google qui, en février 2025, a discrètement renoncé à l'un de ses principes éthiques qui rejetait le développement « d'armes ou technologies [...] visant à blesser des personnes » avant d'obtenir un contrat avec le Pentagone quelques mois plus tard⁸. Ainsi également de Meta, qui s'est associé en mai 2025 au fabricant de systèmes autonomes Anduril pour concevoir des casques de réalité augmentée destinés à « fournir aux combattants une perception accrue et un meilleur contrôle des plateformes sur le champ de bataille⁹ ». Ainsi, toujours, d'Anthropic, d'xAI et d'OpenAI qui, en juin de la même année, ont chacun remporté des contrats de 200 millions de dollars (170 millions d'euros) pour « développer des capacités d'IA avancées » pour le DoD¹⁰. Ces montants se doublent d'un entrisme assumé, qui aboutit à des nominations toujours plus fréquentes d'anciens militaires au sein des entreprises technologiques et de figures du secteur au sein de l'armée américaine¹¹.

7. « Defence Tech Is Blowing Up Silicon Valley's Beliefs », *The Economist*, 13 février 2025. Le terme de *DefTech* désigne les entreprises — dont bon nombre sont des 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. Voir A. Papaemmanuel et L. 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.

8. P. Dave et C. Haskins, « Google Lifts a Ban on Using Its AI for Weapons and Surveillance », *Wired*, 4 février 2025.

9. H. Somerville, « Meta Fired Palmer Luckey: Now, They're Teaming up on a Defense Contract », *The Wall Street Journal*, 29 mai 2025.

10. « US Defense Department Awards Contracts to Google, Musk's xAI », Reuters, 14 juillet 2025.

11. À défaut de pouvoir dresser un tableau parfaitement exhaustif de ces circulations, un premier aperçu des transferts depuis le Congrès américain vers l'industrie militaire est consultable dans J. Mecklin, « The Defense Revolving Door, Silicon Valley Edition », *Bulletin of the Atomic Scientists*, 17 août 2026.

En Europe aussi, la défense a le vent en poupe chez les entreprises de la *tech*. Dès février 2025, l'entreprise française Mistral AI annonçait un partenariat avec Helsing¹², spécialisé dans l'IA embarquée dans les systèmes d'armes, puis avec l'Agence ministérielle pour l'IA de défense (AMIAD) début février 2026¹³. Le 14 avril 2026, Arthur Mensch posait fièrement aux côtés de la ministre des Armées Catherine Vautrin, à l'Hôtel de Brienne. En dépit de son dynamisme, l'écosystème européen demeure toutefois sous la menace d'une dépendance structurelle vis-à-vis d'acteurs américains, qui dominent jusqu'ici très largement le marché.

Le rapprochement global entre acteurs du numérique et institutions militaires ne se fait cependant pas sans heurt. Pour les États, cette imbrication croissante soulève des enjeux de dépendance, d'affaiblissement structurel des capacités et, *in fine*, de souveraineté. Le 4 mars 2026, Anthropic était ainsi désigné comme un « risque pour la chaîne d'approvisionnement de la sécurité nationale des États-Unis », au terme d'un bras de fer entre son patron Dario Amodei et le secrétaire à la Guerre américain, Pete Hegseth, sur les lignes rouges associées à l'utilisation des modèles d'IA de l'entreprise à des fins militaires¹⁴. Quelques semaines plus tard, plusieurs centaines d'employés de Google se fendaient d'une pétition pour que soit rejeté le partenariat de la firme en matière d'IA avec le Pentagone, signe que la révolution culturelle n'est pas tout à fait achevée¹⁵. Bien qu'elles puissent sembler anodines, ces résistances soulignent combien l'alignement de ces entreprises sur des intérêts régaliens peut aussi les conduire à s'exposer, avec le risque de se laisser entraîner par des décisions politiques qui leur échappent.

Comment expliquer ce bouleversement, tant dans l'écosystème américain qu'en Europe, et quelles en sont les répercussions ? Pour répondre à cette question, cette étude reviendra, dans un premier temps, sur la généalogie de l'imbrication entre la *tech* et les armées, afin d'analyser le retournement observé ces dernières années. Enfin, seront examinées ses conséquences sur la souveraineté technologique, l'autonomie stratégique et les capacités militaires européennes.

12. A. Piquard et O. Pinaud, « Accord entre Mistral et Helsing : “Dans l'IA, les Européens ont toutes leurs chances” », *Le Monde*, 20 février 2025.

13. L. Corot, « L'armée française signe un contrat de trois ans avec Mistral AI pour utiliser ses solutions d'IA générative », *L'Usine nouvelle*, 28 mars 2026.

14. R. Bellan, « DoD Says Anthropic's “Red Lines” Make It “Unacceptable Risk to National Security” », *TechCrunch*, 18 mars 2026.

15. G. De Vynck, « Google Workers Petition CEO to Refuse Classified AI Work with Pentagon », *The Washington Post*, 27 avril 2026.

Vers un complexe techno-militaire ?

Printemps 2026. À un bout du spectre, Anthropic¹⁶ s'érige en opposant à l'administration Trump II, au terme d'un bras de fer sur les limites à imposer à l'utilisation de ses modèles d'IA – la surveillance de masse aux États-Unis et les armes entièrement autonomes constituant, aux yeux de Dario Amodei, des lignes rouges spécifiques au-delà de la clause autorisant « tout usage légal » voulue par le gouvernement. À l'autre bout du spectre, Palantir¹⁷ publie sur X une version synthétique de l'essai de son co-fondateur et président Alex Karp, *The Technological Republic*, qui prône « une obligation de participer à la défense de la nation¹⁸ » pour les ingénieurs de la Silicon Valley, au nom d'une « dette morale envers le pays qui a rendu son essor possible¹⁹ ».

Ces deux exemples montrent l'ambivalence des liens entre le secteur de la *tech* et les forces armées. Aux États-Unis comme ailleurs, cette imbrication croissante entre grandes entreprises du numérique et appareils de défense redéfinit les rapports entre innovation, puissance économique et stratégie militaire.

Un retour aux sources

Comme le souligne l'historienne Margaret O'Mara, la lune de miel actuelle entre la *tech* et la défense aux États-Unis relève en réalité d'un « retour aux sources²⁰ ». Dans son ouvrage *The Code: Silicon Valley and the Remaking of America*, elle rappelle la manière dont, à partir des années 1950, les programmes d'armement ont très directement permis l'essor de la Silicon Valley²¹. Pour comprendre l'émergence de ce nouveau « complexe techno-militaire », il convient donc d'abord d'en retracer la généalogie.

16. Anthropic est une entreprise américaine d'intelligence artificielle fondée en 2021 par d'anciens chercheurs d'OpenAI, qui développe des modèles d'IA générative. Sa particularité est de mettre fortement l'accent sur la sécurité, l'alignement et le contrôle des systèmes d'IA.

17. Palantir Technologies est une entreprise spécialisée dans l'analyse de données et les logiciels utilisés par les gouvernements, les armées et les services de renseignement. Fondée en 2003 notamment par Peter Thiel et Alex Karp, elle s'est d'abord fait connaître pour ses outils permettant de croiser d'immenses volumes de données afin de détecter des réseaux terroristes ou criminels après les attentats du 11 septembre 2001.

18. Palantir, « Because We Get Asked a Lot—The Technological Republic, in Brief », X, 18 avril 2026, disponible sur : x.com.

19. *Ibid.*

20. Cité dans A. Piquard, « La Silicon Valley prend un virage militaire inédit, de Google à Palantir », *Le Monde*, 6 septembre 2025.

21. M. O'Mara, *The Code: Silicon Valley and the Remaking of America*, New York, Penguin Press, 2020.

Des relations historiquement symbiotiques

Assiste-t-on à un simple retour en arrière ou à un véritable point de bascule ? En réalité, si les liens actuels entre la *tech* et les armées renouent avec une origine largement oubliée, c'est son degré d'accélération et d'intensité qui constitue la véritable nouveauté, amplifiée par le renforcement des tensions géopolitiques à l'échelle globale. Encore faut-il, pour en prendre la mesure, restituer la profondeur historique d'une relation que le récit contre-culturel de la Silicon Valley a voulu effacer.

En effet, la Silicon Valley n'est pas née dans un garage de Palo Alto, mais dans les laboratoires financés par les États-Unis pendant la Seconde Guerre mondiale et la guerre froide²². Sa figure tutélaire est Frederick Terman, doyen de l'ingénierie à Stanford, qui avait dirigé pendant la guerre le Radio Research Laboratory de Harvard²³ (dont les 800 chercheurs travaillaient sur la guerre électronique). De retour en Californie, son objectif a été d'arrimer durablement son université à la commande militaire, en recrutant d'anciens membres de son laboratoire et en créant un Electronics Research Lab financé par l'Office of Naval Research, l'Air Force et l'Army Signal Corps. À la fin des années 1960, 35 % des financements de recherche en électronique de Stanford provenaient ainsi de contrats classifiés, et la moitié de l'activité du Stanford Research Institute émanait du DoD²⁴. C'est ce qui a rendu possible l'éclosion des premières entreprises de la région : Hewlett-Packard, encouragée par Terman, mais aussi Varian Associates, qui produisait des klystrons pour les radars militaires, ou encore Lockheed Missiles and Space Company, qui était, avant l'essor de l'informatique personnelle, le premier employeur du comté de Santa Clara²⁵.

L'invention même qui a donné son nom à la vallée procède de cette dynamique. En effet, à la fin des années 1950, le transistor supplante peu à peu le tube à vide et bouleverse l'industrie électronique, ce qui pose un problème inédit. Plus les circuits gagnent en puissance, plus le câblage entre composants devient inextricable. Chez Texas Instruments, l'ingénieur Jack Kilby a l'idée, plutôt que de relier des éléments fabriqués séparément, de les réunir dans un même bloc de matériau semi-conducteur. En 1958 naît ainsi le circuit intégré, que l'on appellera bientôt « puce ».

Cette percée doit beaucoup aux liens tissés entre recherche militaire et industrie privée. L'entreprise Texas Instruments, bien qu'initialement fondée pour produire des équipements utilisant les ondes sismiques afin que les pétroliers sachent où forer, a été réquisitionnée pendant la Seconde

22. Ce lien initial dépasse d'ailleurs largement la seule question du financement mais concerne également les commandes, les réquisitions pendant la guerre, le personnel, etc. Voir L. Weiss, *America Inc.? Innovation and Enterprise in the National Security State*, Ithaca, Cornell University Press, 2014.

23. R. S. Lowen, *Creating the Cold War University: The Transformation of Stanford*, Berkeley, University of California Press, 1997.

24. « At the Hands of the Radicals », *Stanford Magazine*, février 2009.

25. L. Weiss, *America Inc.?, op. cit.*

Guerre mondiale par la marine américaine pour fabriquer des sonars permettant de suivre les sous-marins ennemis²⁶. Un an plus tôt, en Californie, huit ingénieurs (les « huit traîtres ») avaient quitté le laboratoire de William Shockley (ancien directeur d'un groupe d'évaluation des systèmes d'armes au Pentagone), pour fonder Fairchild Semiconductor.

C'est à partir de cet écosystème entrepreneurial que prend forme la Silicon Valley. Or, les applications les plus exigeantes des semi-conducteurs concernent alors le guidage des missiles balistiques, les programmes spatiaux et certains systèmes militaires²⁷. Le silicium de la Silicon Valley est donc d'abord un silicium militaire²⁸.

Ce lien originel s'est prolongé, une génération plus tard, dans l'infrastructure numérique elle-même²⁹. L'ancêtre d'Internet, l'ARPANET, a été conçu et financé à partir de 1969 par la Defense Advanced Research Projects Agency (DARPA)³⁰, l'agence de recherche avancée du Pentagone, de même que le système GPS ou les protocoles fondamentaux du réseau. Même les travaux de thèse de Sergey Brin et Larry Page à Stanford, dont est directement issu l'algorithme de Google, ont été financés par une bourse du programme de bibliothèques numériques de la National Science Foundation et de la DARPA³¹.

À la fin des années 1990, la Central Intelligence Agency (CIA) a par ailleurs créé Peleus, une entité à but non lucratif appelée à capitaliser sur les innovations développées dans le secteur privé, et tout particulièrement dans la Silicon Valley. Le choc sécuritaire post-11 septembre 2001 a largement contribué à en renforcer la portée, et le financement de Palantir par ce biais à partir de 2003 n'y est pas étranger. La structure, devenue un fonds de capital-risque interne, a par la suite été rebaptisée In-Q-Tel et s'est vue dotée d'un budget de 37 millions de dollars dès 2005. En 2014, il a atteint les 94 millions de dollars, réalisant 325 investissements dans diverses entreprises technologiques³². Le Pentagone a ensuite créé un instrument similaire en 2015, la Defense Innovation Unit Experimental (DIUx/DIU), tandis que l'année suivante le Defense Innovation Board (DIB) a été mis en place pour servir d'interface entre la Silicon Valley et les autorités politico-militaires.

26. Après la guerre, les dirigeants de Texas Instruments se sont d'ailleurs rendu compte que leur expertise dans le domaine de l'électronique pouvait avoir de nombreuses autres applications militaires. Voir C. Miller, *Chip War: The Fight for the World's Most Critical Technology*, New York, Simon & Schuster, 2022.

27. *Ibid.*

28. K. Flamm, *Creating the Computer: Government, Industry and High Technology*, Washington D.C., The Brookings Institution, 1988.

29. C. Brose, *The Kill Chain: Defending America in the Future of High-Tech Warfare*, New York, Hachette Books, 2022.

30. G. R. Fong, « ARPA Does Windows: The Defense Underpinning of the PC Revolution », *Business and Politics*, vol. 3, n° 3, 2001, p. 213-237.

31. J. Nesbit, « Google's True Origin Partly Lies in CIA and NSA Research Grants for Mass Surveillance », *Quartz*, 7 décembre 2017.

32. D. Paletta, « The CIA's Venture-Capital Firm, Like Its Sponsor, Operates in the Shadows », *The Wall Street Journal*, 30 août 2016.

Loin d'être une singularité américaine, cette généalogie éclaire au contraire un phénomène plus général. Les écosystèmes technologiques les plus dynamiques se sont presque tous constitués à l'ombre d'un appareil de défense. En Israël, les unités technologiques d'élite de l'armée – au premier rang desquelles l'unité 8200, spécialisée dans le renseignement d'origine électromagnétique – irriguent depuis des décennies l'écosystème des startups, dont nombre de fondateurs sont d'anciens réservistes³³. En Chine, la stratégie de « fusion civilo-militaire » érigée en priorité nationale sous Xi Jinping vise explicitement à abolir la cloison entre innovation commerciale et modernisation militaire, en organisant la circulation des données, des capitaux et des personnels entre les deux sphères³⁴. Que le modèle chinois soit lui-même, pour partie, inspiré des initiatives américaines en dit long sur l'universalité du phénomène. La constitution d'une base technologique de pointe et celle d'une puissance militaire procèdent en cela d'un même mouvement.

Un phénomène de « revolving doors »

L'imbrication entre les secteurs technologiques et militaires s'explique également par de nombreuses circulations d'acteurs entre ces deux sphères. Si ces pratiques dites de « *revolving doors* » ne sont pas nouvelles et s'inscrivent dans le temps long, en particulier aux États-Unis³⁵, elles se sont néanmoins multipliées au cours des deux dernières décennies, encouragées par l'efficacité d'organes de lobbying facilitateurs de rencontres³⁶. Le cas le plus connu d'un passage du secteur de la *tech* vers les affaires militaires est sans doute celui d'Eric Schmidt. Cet ancien P.-D. G. de Google (2001-2011), et membre du conseil d'administration de sa maison-mère Alphabet (2015-2017), a exercé une forte influence auprès de l'administration Obama sur les questions d'innovation en termes de défense, avant de présider par la suite le DIB entre 2017 et 2020, et la National Security Commission on Artificial Intelligence de 2018 à 2021. La figure de Doug Beck, ancien militaire et ex-vice-président d'Apple, directeur de la DIU entre 2023 et 2025, est également emblématique.

Tout récemment, on peut aussi mentionner la nomination spectaculaire de quatre figures majeures de la *tech* – avec le grade de lieutenant-colonel – à la tête du Detachment 201, une unité de réserve

33. A. Egozi, « White House Pressuring Israel to Cut Research Ties with China over Dual-Use Concerns », *Breaking Defense*, 29 septembre 2022.

34. E. B. Kania et L. Laskai, « Myths and Realities of China's Military-Civil Fusion Strategy », Center for a New American Security (CNAS), 28 janvier 2021, disponible sur : www.cnas.org.

35. A. Coveri *et al.*, « Big Tech and the US Digital-Military-Industrial Complex », *Intereconomics*, vol. 60, n° 2, 2025, p. 81-87.

36. Le Reagan National Defense Forum constitue ainsi, depuis 2013, un rendez-vous régulier du secteur de la défense au sein duquel les acteurs technologiques ont le vent en poupe. Moins connu, le Silicon Valley Defense Group, groupe informel formé en 2015 et structuré en organisme à but non lucratif à partir de 2020, s'est donné pour mission d'offrir aux dirigeants de sociétés de capital-risque l'occasion de rencontrer officieusement des responsables du Pentagone et des membres du Congrès afin d'en faciliter les rapprochements.

ayant pour mission de combler le fossé technologique entre les secteurs commercial et militaire³⁷. Cette incorporation au sein des forces armées marque un tournant au moins symbolique, faisant passer ces hommes de partenaires civils à officiers supérieurs.

Dans l'autre sens de circulation, les exemples sont aussi nombreux. L'ancien directeur exécutif du DIB, Josh Marcuse (2016-2020), a ainsi pris un poste au sein de Google Public Sector, tandis que l'ancien membre républicain du Congrès, Mike Gallagher, est devenu directeur des opérations de défense chez Palantir en août 2024. Pour ce qui est des militaires de carrière, le général Keith Alexander, ancien directeur de la National Security Agency (NSA) de 2005 à 2014 et du *Cyber Command* de 2010 à 2014, a rejoint le conseil d'administration d'Amazon, tandis que le général Paul M. Nakasone, qui occupait les mêmes postes entre 2018 et 2024, est dorénavant membre du conseil d'administration d'OpenAI. Ces pratiques ont également cours en Europe, où un certain nombre de startups de la *DefTech* (Quantum Systems, Cybsafe, ARX...) ont été fondées par d'anciens militaires³⁸.

Là où ils rejoignaient autrefois des entreprises traditionnelles de la Base industrielle et technologique de défense (BITD), les généraux à la retraite et les hauts responsables du Pentagone quittant leurs fonctions semblent aussi se tourner à présent vers des sociétés de capital-risque investissant dans la défense³⁹. Directement intéressés par les bénéfices des sociétés qui les recrutent sans pour autant en être salariés, ces transfuges participent activement au renforcement des liens avec les décideurs et à la promotion des entreprises que leurs fonds soutiennent⁴⁰.

37. Adam Bosworth (directeur technologique de Meta), Kevin Weil (chef de produit chez OpenAI), Shyam Sankar (directeur technologique chez Palantir) et Bob McGrew (ex-Palantir, ex-OpenAI). Voir « Army Launches Detachment 201: Executive Innovation Corps to Drive Tech Transformation », U.S. Army Public Affairs, 13 juin 2025, disponible sur : www.army.mil.

38. Pour une liste partielle de celles-ci, voir « What Are Some of the European Defence Startups Founded by Military Vets? », Reuters, 4 septembre 2025.

39. En 2023, le *New York Times* identifiait pas moins de 50 figures militaro-sécuritaires de premier plan ayant rejoint des sociétés de capital-risque ou de capital-investissement spécialisées dans le secteur. L'ancien secrétaire à l'Armée, Ryan McCarthy, et Sally Donnelly, ancienne responsable du Department of Defense, ont pris des postes chez Pallas Ventures ; l'ex-conseiller à la sécurité nationale H. R. McMaster est conseiller principal chez Shield Capital, société de capital-risque co-dirigée par Raj Shah, lui-même ancien chef de la DIUx (siégeant par ailleurs au sein d'une commission nommée par le Congrès et chargée d'étudier les moyens de réformer le processus budgétaire du Pentagone) et qui compte également dans ses rangs Michael Brown, successeur de R. Shah à la DIUx ; Nick Sinai, ancien responsable de la Maison-Blanche sous Obama, est aujourd'hui investisseur en capital-risque chez Insight Partners ; Mark Esper, ancien secrétaire à la Défense sous l'administration Trump I, représente Red Cell VC ; le général David Petraeus, ex-directeur de la CIA, est devenu *partner* chez KKR ; Doug Philippone, ancien *ranger* de l'armée américaine, est désormais co-fondateur de Snowpoint Ventures ; Chris O'Donnell, ancien membre des Navy SEALs, dirige Franklin Venture Partners (Air Space Intelligence, Cesium Astro), qui compte parmi ses membres Sam Gray, ancien responsable des acquisitions au Pentagone. Voir E. Lipton, « New Spin on a Revolving Door: Pentagon Officials Turned Venture Capitalists », *The New York Times*, 30 décembre 2023.

40. Notons que de telles proximités ne sont pas sans soulever des interrogations quant aux potentiels conflits d'intérêts susceptibles d'animer ces transfuges. En même temps qu'il exerçait ses responsabilités publiques, Eric Schmidt était à la tête de l'America's Frontier Fund (dans lequel investit aussi Peter Thiel) et du Special Competitive Studies Project, en plus de détenir White Stork, une entreprise de drones militaires.

Ces circulations ont des conséquences directes sur la politique du Pentagone, qui intègre de plus en plus des processus et des modes de pensée issus de la Silicon Valley – rapidité, passage à l'échelle, juste à temps de la chaîne logistique, appétit pour le risque et la révolution technique⁴¹. Là où les organisations militaires et les gouvernements dictaient traditionnellement le rythme et la nature des innovations technologiques, ces dernières sont ainsi de plus en plus déterminées par les startups et leurs bailleurs de fonds. Ceci se reflète jusque dans les structures administratives et les discours officiels⁴², ce qui n'est pas sans conséquences sur la conduite ultérieure d'opérations menées au tamis de ces nouveaux réflexes et outils – en témoigne l'opération *Epic Fury* contre l'Iran, sur laquelle nous reviendrons.

Ces « *revolving doors* » influencent également les priorités et postures des entreprises de la *tech*, en alignant leurs intérêts avec ceux de l'administration fédérale. Sous l'impulsion de Karen Dahut, ancienne de l'US Navy et patronne du « secteur public » (les contrats passés avec l'État fédéral) chez Google, l'entreprise est ainsi revenue sur certains de ses engagements initiaux, dont celui de ne pas œuvrer au développement d'armes⁴³.

Un nouveau cycle de l'innovation

Si ce rapprochement entre la *tech* et les armées relève donc d'un « retour aux sources », il s'opère toutefois dans un cadre transformé. La logique de la guerre froide, qui voyait la puissance publique innover pour le compte des armées puis le secteur commercial civil en recueillir les retombées, a profondément évolué.

Alors que la période 1940-1990 a été largement caractérisée par un modèle de diffusion de la « *MilTech* » vers les usages civils, dans lequel les investissements publics et militaires jouaient un rôle moteur dans le développement de technologies ensuite commercialisées dans le secteur civil, la période 2000-2020 voit s'affirmer une dynamique inverse, de la technologie civile vers la technologie militaire. Ce renversement s'explique notamment par l'ampleur prise par la révolution numérique et l'essor d'Internet, des grandes plateformes technologiques et, plus largement, des entreprises du numérique.

41. Comme en témoigne par exemple un récent rapport du Defense Innovation Board, « *Aligning Incentives to Drive Faster Tech Adoption* », 9 juillet 2024.

42. Le Pentagone s'est doté en décembre 2024 d'une AI Rapid Capabilities Cell, organe ayant pour mission d'intégrer rapidement l'IA générative dans ses opérations militaires et sa gestion administrative. Avec un budget de 100 millions de dollars sur deux ans, ce programme prévoit le développement de projets pilotes, la création d'environnements de test (*sandboxes*) et le financement de solutions issues du secteur privé.

43. E. Woo, « Google and Pentagon Discuss Classified AI Deal as Company Rebuilds Military Ties », *The Information*, 18 avril 2026.

Les capacités de recherche et développement du secteur civil ont en effet atteint des niveaux sans commune mesure avec ceux de la plupart des programmes militaires. À titre de comparaison, le budget annuel de la DARPA, de l'ordre de quelques milliards de dollars, demeure très inférieur aux montants consacrés à la R&D par les principales entreprises technologiques mondiales, dont les investissements se chiffrent individuellement en dizaines de milliards de dollars. Dans ce contexte, les forces armées ne constituent plus le principal foyer d'innovation technologique. Elles sont au contraire confrontées à la nécessité d'identifier, d'intégrer et de capter des innovations issues d'écosystèmes civils dont le rythme de développement et les capacités d'investissement excèdent largement ceux de la recherche militaire. L'essor des stratégies de captation de l'innovation civile doit ainsi être compris moins comme un phénomène conjoncturel que comme la conséquence d'une transformation de l'économie de l'innovation technologique. Or, cette inversion du cycle de l'innovation donne à voir une dualité si généralisée qu'elle brouille la distinction même entre technologie civile et technologie militaire.

De la tech civilianisée à la tech militarisée

Pour comprendre le virage militaire actuellement opéré par l'industrie technologique, il faut revenir sur la dynamique entre innovation civile et innovation militaire. Pendant la guerre froide, la ligne était claire : la puissance publique finançait la recherche de rupture pour des applications militaires, qui donnaient *in fine* lieu à des retombées civiles. De ce fait, de nombreuses avancées technologiques ont vu le jour dans la sphère militaire. C'est le cas, par exemple, d'Internet, du système GPS ou de l'IA. La logique était celle du *spin-off*, où les armées innovaient et le secteur privé commercialisait.

Dans un essai prémonitoire paru en 2001, le futur secrétaire à la Défense Ash Carter, alors professeur à Harvard, annonçait toutefois que : « les innovations de défense de demain seront largement des dérivés de technologies développées et commercialisées par des entreprises privées pour des motifs commerciaux⁴⁴ ». Quatorze ans plus tard, à la tête du DoD, il fondait au cœur de la Silicon Valley la DIUx, avec pour mission explicite de « percer des trous dans le mur » entre le Pentagone et l'écosystème technologique privé⁴⁵, entérinant de fait l'incapacité du DoD à innover seul suffisamment rapidement.

À cela s'ajoute une accélération du rythme de l'innovation, qui rend les cycles d'acquisition militaires traditionnels structurellement obsolètes. En effet, là où les grandes plateformes d'armes – avions de chasse, chars, sous-

44. A. Carter, M. Lettre et S. Smith, « Keeping the Technological Edge », in A. Carter et J. White (dir.), *Keeping the Edge: Managing Defense for the Future*, Cambridge (MA), MIT Press, 2001, p. 129-163.

45. Cité dans S. Winter-Levy, « Silicon Valley Hasn't Revolutionized Warfare — Yet », *Foreign Policy*, 20 septembre 2024.

marins – étaient historiquement développées sur des décennies, les technologies numériques sont mises à jour presque quotidiennement.

La révolution des drones en Ukraine en offre l'illustration la plus saisissante. Des drones commerciaux, disponibles pour quelques centaines de dollars sur des plateformes grand public, ont ainsi été transformés en armes létales par des ingénieurs civils et des soldats astucieux en l'espace de quelques semaines, sans programme étatique ni cahier des charges militaire⁴⁶. En avril 2024, un responsable de l'OTAN estimait dans *Foreign Policy* que certains de ces engins à moins de 1 000 dollars avaient détruit les deux tiers des chars russes perdus depuis le début de la guerre, dont chacun valait plusieurs millions de dollars⁴⁷. Un rapport publié en février 2025 par le Royal United Services Institute (RUSI) indique encore que les drones sont responsables de 70 à 80 % des pertes sur le champ de bataille⁴⁸. La puissance de feu n'est par conséquent plus le monopole de systèmes d'armes sophistiqués issus de décennies de R&D étatique, mais elle est désormais accessible « sur étagère ».

Ce phénomène de *spin-in* redéfinit en profondeur les termes de la relation entre entreprises technologiques et institutions militaires. Il ne s'agit plus seulement d'opportunités commerciales pour les premières, ou de commodités pour les secondes, mais bien d'une dépendance structurelle. Comme le formulait sans ambages Antonio Missiroli dans la *Revue de l'OTAN*⁴⁹ en 2020 :

« L'investissement dans la science et la technologie est à présent principalement déterminé par les marchés commerciaux, au niveau tant national que mondial, et l'importance des dépenses d'investissement est sans commune mesure avec celles spécifiquement consacrées à la défense, si bien que, dans certains domaines technologiques, la défense repose entièrement sur l'évolution de la société civile et des marchés. »⁵⁰

C'est à cette aune que doit être examinée la hausse spectaculaire du budget de la DIU. De 191 millions de dollars en 2023, il est passé à près d'un milliard (983 millions) pour l'exercice budgétaire 2024, soit une augmentation de plus de 400 % en un an, voulue par le Congrès, qui signifiait ainsi son impatience face à la lenteur d'adoption des technologies

46. T. Jankowski, « La prolifération des drones civils militarisés en Ukraine : une école de guerre pour les états-majors occidentaux », *Le Rubicon*, 20 avril 2023.

47. J. Detsch, « Ukraine's Cheap Drones Are Decimating Russia's Tanks », *Foreign Policy*, 9 avril 2024.

48. « Tactical Developments During the Third Year of the Russo-Ukrainian War », Royal United Services Institute (RUSI), février 2025, disponible sur : www.rusi.org.

49. La *Revue de l'OTAN* (*NATO Review*) est la publication éditoriale en ligne de l'Organisation. Ce n'est pas une revue académique mais un magazine institutionnel publié par l'OTAN elle-même, qui diffuse des articles d'analyse et d'opinion sur les questions de sécurité et de défense.

50. A. Missiroli, « Game of Drones? Ou comment les nouvelles technologies influent sur la dissuasion, la défense et la sécurité », *Revue de l'OTAN*, 5 mai 2020, disponible sur : <https://archives.nato.int>.

commerciales par le Pentagone⁵¹. Ce budget s'est ensuite maintenu à hauteur de 979 millions sous l'administration Trump II, signe de l'entérinement de cette évolution⁵².

Le financement massif d'une institution dont la vocation est précisément de faire entrer des produits civils dans l'arsenal militaire témoigne, là encore, du « virage » en cours. Ce n'est pas donc uniquement la *tech* qui se militarise par vocation, mais aussi la défense qui se trouve dans l'obligation de se « technologiser » pour rester compétitive. Le rapprochement entre ces deux mondes est donc, à bien des égards, la réponse tardive et parfois chaotique d'une institution militaire rattrapée par une innovation technologique de rupture qu'elle ne conduit plus, et par conséquent ne maîtrise plus.

Un antimilitarisme de façade ?

Au tournant des années 2010, pourtant, le secteur de la *tech* affichait une réticence à se « compromettre » avec celui de la défense. Cette posture s'enracinait dans le récit que les acteurs de la Silicon Valley aimaient faire de leurs propres origines. Celui-ci était empreint de la contre-culture héritée des communautés californiennes des années 1960, où l'ordinateur personnel était envisagé comme un outil d'émancipation individuelle arraché aux mains de l'État⁵³. Le Léviathan de cette mythologie se voyait ainsi destitué des outils d'origine militaire – au premier rang desquels l'informatique – pour en faire des plateformes de créativité et d'expression personnelle. Google, la firme emblématique de cette génération, avait résumé cet *ethos* dans une devise restée célèbre : « *Don't be evil* ».

Bien que ce récit fondateur relève largement du mythe, il a alimenté une véritable culture d'entreprise, dont les effets se sont manifestés avec éclat au printemps 2018. En avril, des journalistes révèlent en effet que Google participe au projet Maven, un programme du Pentagone visant à exploiter l'IA pour analyser les images captées par les drones militaires. 4 600 employés signent alors une pétition adressée au P.-D. G., Sundar Pichai, et une douzaine de salariés démissionnent en signe de protestation. Le texte de la pétition est particulièrement critique, indiquant que « Google ne devrait pas être dans le business de la guerre ». Les salariés y mettent aussi en avant le risque de « salir l'image de marque de Google et son attractivité auprès des talents⁵⁴ » alors que l'entreprise lutte déjà pour conserver la confiance du public « au milieu de peurs grandissantes sur les biais et la militarisation de l'intelligence

51. C. Albon, « Defense Innovation Unit Would Get Major Funding Boost in Spending Bill », *Defense News*, 21 mars 2024.

52. Office of the Under Secretary of Defense (Comptroller), *Defense Budget Overview: Fiscal Year 2026 Budget Request*, Department of Defense, juillet 2025, disponible sur : <https://comptroller.defense.gov>.

53. A. Bradford, *Digital Empires: The Global Battle to Regulate Technology*, New York, Oxford University Press, 2023.

54. Cité dans P. Montet, « Refusant de travailler avec le Pentagone, des salariés de Google démissionnent », *Usbek & Rica*, 16 mai 2018.

artificielle ». Les signataires exigent non seulement l'abandon du contrat, mais également que soit adoptée une politique excluant explicitement toute participation, présente ou future, à des technologies d'armement.

Le succès de la mobilisation est à l'époque spectaculaire. Google laisse expirer le contrat Maven – pourtant estimé à près de 250 millions de dollars – en 2019 et publie une charte de principes sur l'IA, s'engageant à ne pas développer d'armes ni de technologies de surveillance. La portée de la pétition dépasse d'ailleurs rapidement Google et inaugure une vague de mobilisations similaires dans tout le secteur⁵⁵. Le vocabulaire utilisé – refus de la « létalité », exigence d'un « droit de regard » des ingénieurs sur l'usage de leur travail – dessine alors les contours d'une conscience professionnelle qui se veut en surplomb des intérêts régaliens.

Les auteurs Fred Turner et Yasha Levine, qui ont consacré des travaux à la culture de la Silicon Valley, soulignent néanmoins le caractère illusoire de cette prétendue rupture, tant la coopération entre les entreprises technologiques et le DoD est constitutive de l'histoire de la Silicon Valley, depuis les financements fédéraux de la guerre froide jusqu'à la DARPA⁵⁶. S'il salue le courage des employés démissionnaires, Yasha Levine observe également que ce qui rendait le projet Maven scandaleux aux yeux des salariés n'était pas tant le lien avec l'armée en soi que sa visibilité – le drone étant perçu comme directement connecté au champ de bataille, là où le financement militaire d'autres recherches s'avère moins tangible⁵⁷.

L'ambivalence de cette industrie née de la guerre mais ayant bâti son image publique sur le refus de celle-ci explique probablement la rapidité du retournement actuel, tout autant que la part grandissante des contrats publics dans le chiffre d'affaires de ces entreprises. Dès lors que le contexte stratégique et financier l'a justifié, la *tech* a pu renouer ouvertement avec ses origines militaires sans avoir, au fond, à se renier véritablement.

Des technologies duales par nature

La notion de « dualité », qui renvoie à l'idée qu'un même objet peut servir à la fois des fins civiles et militaires, a longtemps constitué un outil d'analyse précieux en même temps que le socle de tout un édifice normatif (sur lequel reposent les régimes de contrôle des exportations, les listes de biens à double usage ou encore l'arrangement de Wassenaar). Or, cette notion repose sur le présupposé qu'une distinction entre un usage pacifique et une application militaire est possible. C'est précisément ce postulat que les technologies numériques, en particulier l'IA, rendent caduc. Parce que la plupart des applications d'IA sont potentiellement duales, le critère de la « dualité » perd l'essentiel de son pouvoir discriminant. Celle-ci ne désigne en effet plus une

55. N. Tiku, « The Year Tech Workers Realized They Were Workers », *Wired*, 24 décembre 2018.

56. K. Kokalitcheva, « Turner: Silicon Valley's Military Work Shouldn't Be a Surprise », *Axios*, 29 mai 2018.

57. N. Tiku, « The Line Between Big Tech and Defense Work », *Wired*, 21 mai 2018.

sous-catégorie de technologies sensibles, mais la condition ordinaire de l'innovation.

De fait, les systèmes d'armes contemporains, y compris les plus sophistiqués, procèdent rarement d'un effort de recherche militaire « pur », mais résultent le plus souvent de développements civils ultérieurement intégrés à des applications de défense. Dans le champ de l'IA en particulier, le secteur civil occupe la pointe de l'innovation, tandis que les armées en sont réduites à adapter à leurs besoins des modèles conçus pour le marché.

L'usage du modèle de langage Claude d'Anthropic par Palantir *via* le *Maven Smart System* dans le cadre de l'opération *Epic Fury* contre l'Iran au printemps 2026 témoigne de cette dynamique. Claude n'a pas été conçu comme un outil militaire ; c'est un modèle de langage généraliste, commercialisé pour des usages civils. Il s'est pourtant retrouvé au cœur d'une opération militaire d'envergure⁵⁸. Un outil pensé pour le grand public s'est ainsi révélé un instrument stratégique, sans qu'aucune intention militaire n'ait présidé à sa conception.

Se pose alors la question du droit de regard. Qui, de celui qui conçoit une technologie ou de celui qui l'emploie, doit décider de ce à quoi elle peut légitimement servir ? Cette question travaille la communauté des chercheurs en IA depuis plus d'une décennie. Dès 2015, une lettre ouverte coordonnée par le Future of Life Institute et signée par plusieurs milliers de chercheurs réclamait ainsi l'interdiction des armes autonomes échappant à un contrôle humain significatif. Ils écrivaient ainsi :

« De même que la plupart des chimistes et des biologistes n'ont aucun intérêt à mettre au point des armes chimiques ou biologiques, la plupart des chercheurs en intelligence artificielle n'ont aucun intérêt à développer des armes fondées sur l'IA. Ils ne souhaitent pas non plus que d'autres discréditent leur domaine en le faisant, au risque de susciter une forte réaction de rejet du public envers l'IA, qui pourrait compromettre les bénéfices que cette technologie est susceptible d'apporter à la société à l'avenir. En effet, les chimistes et les biologistes ont largement soutenu les accords internationaux ayant permis d'interdire efficacement les armes chimiques et biologiques, tout comme la majorité des physiciens ont appuyé les traités interdisant les armes nucléaires déployées dans l'espace et les armes à laser conçues pour aveugler. »⁵⁹

En 2018, ces mêmes milieux franchissaient un pas supplémentaire en s'engageant individuellement, par un texte signé notamment par les fondateurs de DeepMind, à ne jamais « participer ni contribuer » au

58. F. Timotija, « Anthropic's Claude Used by Pentagon in War with Iran, Official Confirms », *The Hill*, 24 mars 2026.

59. « Autonomous Weapons: An Open Letter from AI & Robotics Researchers », Future of Life Institute, juillet 2015, disponible sur : <https://futureoflife.org>.

développement, à la fabrication, au commerce ou à l'utilisation d'armes létales autonomes⁶⁰, selon le principe qu'une décision de vie ou de mort ne devrait jamais être déléguée à une machine.

Pour autant, la figure technologique claire posée par ces textes – l'arme autonome ou le « robot tueur » – n'est plus la seule incarnation possible des dérives de l'IA militarisée. Les outils d'IA s'intègrent désormais dans une chaîne d'opérations (analyse du renseignement, identification de cibles, simulation de scénarios) où leur contribution est essentielle, sans être directement létale. Dans ce contexte, l'engagement à ne pas construire d'armes autonomes perd de sa pertinence en même temps que de sa force.

C'est ce qu'illustre la position d'Anthropic face au DoD : Dario Amodei ne rejetait pas toute utilisation militaire de ses modèles, mais souhaitait conserver un droit de regard sur certains usages considérés comme incompatibles avec les valeurs démocratiques des États-Unis. La vive opposition de l'administration à cette revendication montre alors à quel point il est devenu difficile de concilier l'autonomie des entreprises technologiques et les exigences de la libre disposition de la force armée⁶¹.

Cette difficulté est aussi, en dernière instance, d'ordre culturel. Le virage militaire de la *tech* ne se joue pas seulement dans les contrats et les budgets, mais dans un imaginaire professionnel traversé de tensions. L'*ethos hacker*, hérité de la contre-culture, hostile à toute hiérarchie et soupçonneux envers l'État, y coexiste avec un patriotisme décomplexé qui fait de la contribution à la puissance nationale une fierté, et non plus une compromission. C'est entre ces deux pôles que se positionnent aujourd'hui les chercheurs, les ingénieurs, les entreprises et les modèles qu'ils élaborent.

60. « Lethal Autonomous Weapons Pledge », Future of Life Institute, juin 2018, disponible sur : <https://futureoflife.org>.

61. Le principe de libre disposition de la force armée établit que le pouvoir exécutif est le seul décisionnaire en matière de recours à la force.

« We must rebel against the tyranny of the apps »

« Nous devons nous rebeller contre la tyrannie des applications », prêche Alex Karp dans *The Technological Republic*⁶². Cette formule est emblématique du renversement rhétorique actuellement à l'œuvre. Le « business de la guerre » n'est plus envisagé comme une compromission, contrairement au divertissement. L'iPhone et ses applications, autrefois fierté de l'industrie technologique, sont accusés d'avoir « rétréci le sens du possible » d'une génération d'ingénieurs⁶³. Comment des acteurs qui faisaient de la distance à l'égard de la guerre un marqueur identitaire en sont-ils venus à embrasser ce discours ? Ce basculement ne s'explique probablement ni par une conversion morale soudaine ni par le seul appât du gain. Il est le produit d'une conjonction de chocs – sanitaire, géopolitique, budgétaire – et d'un travail idéologique dont il convient de restituer ici la mécanique.

Le double tournant de la pandémie et de l'invasion russe de l'Ukraine

Dans la lignée d'efforts précédents visant à empiéter sur divers domaines régaliens (santé, éducation, transports, diplomatie cyber...), l'intérêt des *Big Tech* pour le secteur de la défense constitue une nouvelle étape. Ces velléités s'étaient déjà en partie révélées lors de la crise provoquée par la pandémie de Covid-19. Les discours d'urgence sanitaire d'alors, rapidement mâtinés de préoccupations d'ordre sécuritaire, ont ouvert des débouchés immédiats pour l'ensemble du secteur de la *tech*. Les multiples espaces ouverts par les gouvernements (collecte et traitement des données de santé, applications de traçage, surveillance et contrôles numériques, etc.) ont ainsi été massivement investis par ces acteurs, qui y ont vu une triple opportunité : diversifier leur modèle d'affaires, imposer leurs solutions logicielles et se racheter une image de marque⁶⁴.

Deux ans plus tard, l'invasion à grande échelle de l'Ukraine en février 2022 a ouvert des perspectives similaires et très largement accéléré l'immixtion du secteur de la *tech* dans la défense. Celui-ci s'est tout d'abord

62. A. Karp et N. Zamiska, *The Technological Republic: Hard Power, Soft Belief, and the Future of the West*, Londres, The Bodley Head, 2025.

63. *Ibid.*

64. B. Pajot et H. Verdier, « Géopolitique d'une pandémie à l'ère numérique », *Enjeux numériques*, n° 14, juin 2021, p. 120-126 ; « Les géants d'Internet réhabilités par la crise du Covid-19 », *Courrier international*, 30 mars 2020.

opportunément porté au secours du gouvernement et des forces armées ukrainiennes, qui, dans les premiers jours de l'invasion, ont ainsi pu bénéficier des technologies des Big Tech (Microsoft, Google et, dans une moindre mesure, Amazon et Meta) qui ont rapidement rendu disponibles diverses solutions d'urgence (intégration et analyse de données, cyberdéfense, accès au *cloud*...). Le rôle de Starlink pour assurer une connexion satellitaire à l'armée ukrainienne, à la demande de Kiev, s'est également avéré central.

Dans un second temps, l'évolution considérable du champ de bataille engendrée par le retour de la guerre de haute intensité à l'ère du *Big Data* et de l'IA a offert de nouvelles perspectives à de nombreux acteurs. Le recours massif à l'analyse de données, à l'imagerie satellitaire, aux drones et autres systèmes autonomes, en complément ou substitut des armements plus traditionnels a nécessité une agilité et des capacités d'innovation propres à celles des startups. Si l'écosystème *DefTech* préexistait au conflit en cours, il s'est considérablement développé depuis – notamment et logiquement en Ukraine⁶⁵ – pour satisfaire les nouveaux besoins engendrés par ce qui a été qualifié de laboratoire technologique à ciel ouvert⁶⁶. Le conflit est à la fois vecteur d'opportunités économiques et d'une forme de (re)légitimation⁶⁷, en particulier pour tous les acteurs en capacité de démontrer le caractère « *combat proven* » de leurs technologies.

L'avènement d'un « patriotisme *in tech* »

Le virage dont il est ici question a fait de l'engagement au service de la défense un objet de fierté, voire une norme sociale au sein de l'industrie de la *tech*. Alors que les ingénieurs de 2018 exigeaient un droit de retrait, leurs héritiers de 2025 revendiquent désormais un devoir de service. Ce retournement des valeurs, spectaculaire par sa rapidité, s'est incarné dans des gestes symboliques, des prises de position et des dispositifs institutionnels qui témoignent de cette étonnante reconversion morale.

Palmer Luckey, le fondateur d'Anduril, en est l'une des figures majeures dans son expression la plus radicale. Ancien enfant prodige de la réalité virtuelle, écarté de Facebook après avoir soutenu Donald Trump, Palmer Luckey a bâti son entreprise sur la conviction que la modernisation technologique de l'armée est une condition de survie du « mode de vie⁶⁸ » américain. Sa formule selon laquelle les États-Unis doivent cesser d'être « le gendarme du monde » pour en devenir « l'armurerie » atteste d'un

65. M. Newton, « What Makes Ukrainian Defense Technology so Effective? Speed, Scale & Innovation », Center for European Policy Analysis (CEPA), 1^{er} juillet 2026, disponible sur : www.cepa.org.

66. K. Bego, « How a Surge in Defence and Dual-Use Technology Investment Could Reconfigure the Global AI Race », Chatham House, 7 mai 2026, disponible sur : www.chathamhouse.org.

67. Notons que certains d'entre eux, à l'image de Palantir ou de Clearview AI, ont saisi l'occasion de redorer leur image publique, alors ternie par leurs activités menées sur le sol américain.

68. « Palmer Luckey Wants America to Win », entretien de Palmer Luckey, Hoover Institution, mai 2026, disponible sur : www.hoover.org.

patriotisme assumé, qui fait de la vente d'armes un service rendu à la nation et à ses alliés⁶⁹. Interrogé sur les limites qu'il se fixerait, Palmer Luckey revendique une soumission volontaire à la décision politique. La question de savoir à qui vendre des armes relève, selon lui, du choix du gouvernement américain, et non du fabricant.

Le manifeste le plus explicite de ce réengagement est néanmoins venu de Palantir. Dans *The Technological Republic*, paru en 2025, son fondateur Alex Karp adresse à la Silicon Valley une critique cinglante. L'industrie aurait trahi sa vocation en délaissant les grands projets d'intérêt national – la défense et la sécurité en particulier – au profit d'outils futiles destinés à satisfaire les caprices des consommateurs⁷⁰. Alex Karp déplore encore que les esprits les plus brillants, autrefois mobilisés pour des enjeux d'importance nationale, se soient détournés vers le développement d'applications de partage de photos et d'algorithmes marketing.

Il oppose à cette dérive un impératif de reconquête. Selon lui, la Silicon Valley aurait commis l'erreur stratégique de se présenter comme extérieure au pays qui l'a vue naître, alors qu'elle devrait au contraire prendre part à l'« articulation du projet national⁷¹ ». Le livre, décrit comme un « appel aux armes pour les ingénieurs de la Silicon Valley⁷² », a connu un retentissement considérable et nourri un climat idéologique favorable au réarmement de l'industrie technologique.

À ce discours ambiant s'est ajouté, presque simultanément, le dispositif institutionnel inédit qu'a constitué le Detachment 201. Le nom de cette unité – clin d'œil au code de statut HTTP « 201 », qui signale la création réussie d'une ressource sur un serveur – témoigne de l'esprit de la démarche. Loin d'être un geste symbolique isolé, le dispositif semble voué à s'institutionnaliser. En juin 2026, une deuxième cohorte a ainsi prêté serment (composée des dirigeants de Cloudflare et de Sutter Hill Ventures ainsi que du co-fondateur de Facebook AI Research) ; tandis que l'US Army réformait son programme de commissionnement direct – qui permet à des profils civils d'intégrer directement l'armée comme officiers sans suivre le parcours classique de formation – pour ramener le délai d'incorporation de dix-huit à six mois, transformant l'expérimentation en filière pérenne de recrutement des élites technologiques⁷³. Entre-temps, la première cohorte a manifestement conseillé les forces sur des dossiers aussi structurants que les chaînes d'approvisionnement en munitions ou la stratégie en matière de systèmes autonomes.

69. « 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.

70. A. Karp et N. Zamiska, *The Technological Republic*, op. cit.

71. *Ibid.*

72. B. Ivry, « A Call to Arms (Literally) for Tech Bros », *The Washington Post*, 21 février 2025.

73. « US Army Commissions Second Cohort of Tech Executives into Innovation Unit », *Army Times*, 12 juin 2026.

Cette tendance a son pendant européen, quoique sous une forme distincte. En Europe de l'Ouest, l'engagement se pare moins des couleurs nationales que de la défense d'un projet démocratique. Helsing, qui est devenu en quelques années le champion continental de l'IA de la défense, entend mettre ses systèmes « au service de nos démocraties », afin que les sociétés européennes demeurent libres de leurs décisions souveraines et maîtresses de leurs destins⁷⁴. La rhétorique n'est donc pas celle du drapeau national, mais celle des valeurs et de l'autonomie stratégique européennes, qui mobilise d'autant plus que la guerre en Ukraine et le désengagement américain ont ravivé, sur le continent, la crainte de leur vulnérabilité.

Le fait que le milliardaire suédois Daniel Ek, fondateur de Spotify, ait choisi d'investir, via son fonds Prima Materia, 600 millions d'euros dans Helsing, dont il préside le conseil d'administration, en dit long sur le renversement des priorités du capital technologique européen. Sa justification tient en une phrase : l'Europe « doit se défendre technologiquement⁷⁵ ». Helsing est ainsi devenu la première *decacorn* de la défense européenne, aujourd'hui valorisée à 18 milliards d'euros⁷⁶. Daniel Ek a, quant à lui, été la cible d'un boycott d'artistes, dont Massive Attack, qui ont retiré leur musique de Spotify en signe de protestation⁷⁷.

La trajectoire de Quantum Systems illustre, en miroir, la même dynamique. En effet, lorsque l'ancien officier de la Bundeswehr, Florian Seibel, a fondé cette entreprise de drones en 2015, bâtir une société de défense financée par le capital-risque relevait en Europe de la gageure, tant les fonds, corsetés par leurs mandats ESG, excluaient le secteur⁷⁸. Dix ans et 19 000 missions au-dessus de l'Ukraine plus tard, Quantum Systems est devenue la première licorne duale du continent. Après avoir levé 1,2 milliard de dollars en juillet 2026, son fondateur entend désormais bâtir un « *neo prime* » (un nouveau géant de l'armement) appelé à bousculer les industriels historiques⁷⁹.

Bien que dans une moindre mesure, la startup Harmattan AI, co-fondée en 2024 par le franco-marocain Mouad M'Ghari et spécialisée dans la production de drones et de systèmes autonomes de défense, évolue dans une logique similaire. Devenue première licorne française de la

74. Helsing, document de présentation institutionnelle, septembre 2025, disponible sur : <https://helsing.ai>. La formule originale, « Artificial Intelligence to Serve Our Democracies », est le libellé revendiqué de la mission de l'entreprise.

75. C. Loizos, « Spotify's Daniel Ek Just Bet Bigger on Helsing, Europe's Defense Tech Darling », TechCrunch, 16 juin 2025.

76. H. Meddah, « Une valorisation à 18 milliards de dollars : Helsing, preuve que la frénésie des investisseurs pour l'intelligence artificielle fait son entrée dans le secteur de la défense », *L'Usine nouvelle*, 16 juillet 2026.

77. M. Sukherjee, « Spotify Founder Daniel Ek Pivots from Music to European Tech Ventures », Reuters, 1^{er} octobre 2025.

78. A. Férey et L. de Roucy-Rochegonde, « "Don't Bank on the Bombs" : l'industrie de défense face aux nouvelles normes européennes », *Briefings de l'Ifri*, Ifri, 22 septembre 2022.

79. K. Nicol-Schwartz, « Autonomous Drone Startup Quantum Systems Raises \$1.2 Billion as Investors Pile into Defense », CNBC, 2 juillet 2026.

DefTech à la suite de sa dernière levée de fonds (notamment auprès de la BITD nationale), l'entreprise pourrait toutefois souffrir d'évoluer dans un contexte où les commandes étatiques sont jusqu'ici trop faibles pour assurer la pérennité d'un marché hautement concurrentiel⁸⁰.

À l'est de l'Europe, c'est bien la possibilité d'une nouvelle agression russe qui sert de catalyseur, l'écosystème se voyant stimulé par la demande et les incitations étatiques : la part du produit intérieur brut (PIB) dévolue à la défense (autour de 5 %) y est plus élevée que dans le reste de l'Union et contribue à susciter des vocations. Quand Varsovie multiplie les partenariats externes avec des industriels sud-coréens, israéliens et américains, les États baltes intègrent les retours d'expérience ukrainiens et s'associent à des startups américaines, allemandes et britanniques en complément de l'émergence d'acteurs locaux prometteurs⁸¹.

80. Harmattan AI coexiste avec Alta Ares, Egide, Stryx AI ou encore Skydrone Robotics. Voir O. Pinaud, « Derrière l'ébullition dans le secteur des drones militaires en France, une montée en puissance incertaine », *Le Monde*, 7 mai 2026.

81. Tels Skeleton Technologies, Milrem Robotics, RSI Europe, Frankenburg Technologies, SPH Engineering, Origin Robotics ou encore SUBMerge Baltic. Voir T. Vilks et E. Poga, « Inside the Baltic Defence Tech Landscape », Proposal Peak, 30 juin 2026, disponible sur : <https://proposalpeak.com>. Pour un aperçu détaillé de cet écosystème, voir également : <https://app.dealroom.co>.

De la distance affichée au rapprochement assumé

Le 4 février 2025, Google supprimait la section énumérant les « applications qui ne seront pas poursuivies » – au premier rang desquelles les armes et la surveillance – de ses « principes sur l’IA » adoptés en 2018, précisément pour apaiser la fronde interne suscitée par le projet Maven⁸². La direction de la firme de Mountain View s’en est justifiée dans un billet de blog par la nécessité, pour les « démocraties », de « mener le développement de l’IA » et de servir la sécurité nationale⁸³. Après avoir examiné, dans la section précédente, les chocs exogènes ayant conduit à cet élan patriotique dans le secteur de la tech, nous nous intéressons désormais aux motivations profondes des géants du numérique.

L’opportunisme mercantile face à une offre étatique en croissance

Avec le retour de la guerre de haute intensité, et alors que le budget fédéral américain avoisine les 840 milliards de dollars en 2026, le marché militaire et les contrats avec ce qui est devenu le Department of War (DoW) représentent une manne financière d’ampleur. Or, près de 300 milliards de cette somme sont spécifiquement dédiés aux acquisitions et au développement de nouvelles capacités, ce qui profite directement aux entreprises du secteur technologique⁸⁴. Sous l’égide d’une entité dédiée nouvellement créée, le Defense Autonomous Warfare Group (DAWG), l’IA de défense représente ainsi une part non négligeable (13,4 milliards) du budget du DoD et est amenée à croître exponentiellement⁸⁵. L’ambition affichée par l’administration Trump II est ainsi de déployer une doctrine « *AI first* », qui faciliterait pour l’armée américaine l’acquisition et l’intégration rapide d’outils d’IA mais orienterait également la conception et la conduite d’opérations sur le champ de bataille physique comme

82. N. Tiku et G. De Vynck, « Google Drops Pledge Not to Use AI for Weapons or Surveillance », *The Washington Post*, 4 février 2025.

83. D. Hassabis et J. Manyika, « Responsible AI: Our 2024 Report and Ongoing Work », *Blog Google*, 4 février 2025, disponible sur : <https://blog.google>.

84. Le Joint Artificial Intelligence Center (JAIC) est passé de 500 millions de dollars en 2023 à plus de 1,2 milliard en 2025. Voir J. Isler, « DOD AI Initiatives Will Open the Door to New Opportunities », *Washington Technology*, 22 août 2025, et « Defense Tech Trends 2026 », disponible sur : www.clipperdefense.com.

85. Le Pentagone demande ainsi de porter ce financement à 54 milliards de dollars pour le budget 2027. Voir A. Down, « Pentagon Asks for \$54bn in Pivot Towards AI-Powered War », *The Guardian*, 22 avril 2026.

numérique⁸⁶. Cette ambition se voit également renforcée par la *National Security Science & Technology Strategy* (NSSTS) parue en août dernier, qui place l'IA au cœur du développement capacitaire des forces armées⁸⁷.

Le Pentagone n'est néanmoins pas le seul à consentir à des efforts significatifs. La Commission européenne envisage ainsi d'allouer 131 milliards d'euros de son *European Competitiveness Fund* (2028-2034) au bénéfice des secteurs de la défense, de l'espace et de la sécurité⁸⁸, tandis que le plan *ReArm Europe* prévoit un réarmement collectif des États membres à hauteur de 800 milliards d'ici à 2030. La Commission a aussi financé, *via* son Fonds européen de Défense, des projets innovants à hauteur de 6 milliards d'euros depuis 2021 et jusqu'à 2027⁸⁹. Elle vient également de mettre en place le programme « AGILE » à destination de la *DefTech* européenne, doté de 115 millions d'euros pour 2027⁹⁰. Le Fonds européen d'investissement (FEI) déploie, quant à lui, depuis 2024, un programme dédié de 175 millions d'euros⁹¹.

Du côté des États membres, la France a par exemple acté le doublement de son budget d'IA de défense d'ici à 2030 pour atteindre 2 milliards d'euros, principalement dévolus à l'AMIAD⁹², tandis que son Agence d'innovation de défense dispose d'un budget d'1,2 milliard d'euros annuels⁹³. Paris soutient également l'écosystème *via* les fonds « Innovation Défense » de la BPI (275 millions d'euros depuis 2021) et « Émergence Défense » de la Caisse des Dépôts (200 millions levés début 2026, avec un objectif de 400 millions à terme). L'Allemagne a également annoncé en juillet dernier la création d'un fonds d'investissement étatique devant permettre la prise de participations dans la *DefTech* nationale⁹⁴. Hors de l'UE, le Royaume-Uni déploie *via* son fonds d'innovation de défense (UKDI) près de 2 milliards d'euros d'ici à 2030, auxquels s'ajoutent 5 milliards dédiés à l'acquisition de systèmes autonomes et d'armes laser, ainsi que 100 millions pour soutenir la *Rapid AI Delivery Taskforce*⁹⁵.

86. H. Lorber, « The Pentagon's AI-First Doctrine and Its Implications for Modern Warfare: Lessons from the Conflict with Iran », Institute for National Security Studies (INSS), 19 mars 2026, disponible sur : www.inss.org.il.

87. *National Security Science & Technology Strategy*, Washington, D.C., Maison-Blanche, août 2026, disponible sur : www.whitehouse.gov.

88. « The 2028-2034 EU Budget for a Stronger Europe », Commission européenne, 16 juillet 2025, disponible sur : <https://commission.europa.eu>.

89. 70 millions d'euros sont ainsi dévolus à la seule IA de défense pour 2027. Voir « Artificial Intelligence (AI) in Defence », *Factsheet*, Commission européenne, décembre 2025 ; « EDF 2025 Call Results », Commission européenne, 2026, disponibles sur : <https://defence-industry-space.ec.europa.eu>.

90. « AGILE », *Factsheet*, Commission européenne, disponible sur : <https://ec.europa.eu>.

91. A. Pugnet, « Défense : le Fonds européen d'investissement propose 175 millions d'euros pour soutenir les start-up et les PME », Euractiv, 12 janvier 2024.

92. « Défense : la stratégie ministérielle sur l'intelligence artificielle », disponible sur : www.info.gouv.fr.

93. « Les missions de l'Agence », Agence de l'innovation de défense (AID), ministère des Armées, disponible sur : www.defense.gouv.fr.

94. M. Martinez et M. Murray, « Germany to Take Direct Stakes in Defence Startups under New Strategy », Reuters, 22 juillet 2026.

95. Londres prévoit de dépenser 10 % de son budget d'équipement de défense dans les nouvelles technologies (IA, quantique, systèmes autonomes). Voir « The Defence Investment Plan: Funding

De telles perspectives ne peuvent manquer d'aiguiser les appétits et d'encourager un secteur privé sollicité chaque année davantage pour répondre aux objectifs rehaussés des États occidentaux. La vision maximaliste américaine – qui repose sur un récit savamment orchestré sur l'état de crise et l'urgence dans lesquels se trouverait le secteur de la défense face à la perspective d'une confrontation avec la Chine⁹⁶ – contribue à créer un effet d'entraînement global.

Ce récit érige par ailleurs les entreprises de la Silicon Valley en porteuses de solutions agiles et rapidement déployables, ce qui les valorise sur les plans politique et financier. Les contrats publics offrent également une prévisibilité et une stabilité vitales dans un secteur en perpétuelle évolution et soumis à une concurrence féroce en dépit de sa consolidation oligopolistique. Profitant du caractère discrétionnaire des contrats et de la quasi-absence de redevabilité qu'ils impliquent, ces acteurs peuvent capitaliser sur leurs succès commerciaux dans le domaine militaire pour en faciliter d'autres dans le champ sécuritaire civil (police, frontières, renseignement intérieur...), amplifiant ainsi leur emprise financière bien au-delà du seul budget de défense.

Alors que les *Big Tech* étaient les principaux partenaires de l'administration américaine et de sa « guerre contre le terrorisme », cumulant au moins 44 milliards de dollars de contrats entre 2004 et 2021⁹⁷, cette collaboration n'a guère faibli depuis⁹⁸. Palantir (10 milliards de dollars sur dix ans), Oracle (7 milliards), Anduril (près d'un milliard), Google, Anthropic – avant la rupture récente – et xAI (200 millions chacun) comptent ainsi parmi les principaux bénéficiaires de ces trois dernières années⁹⁹. Ce climat économique favorable a, en retour, permis aux startups de la *DefTech* de lever 155 milliards de dollars entre 2021 et 2024, soit près du triple de ce levé sur les quatre années précédentes¹⁰⁰.

Explainer », Ministère de la Défense, disponible sur : www.gov.uk ; House of Commons Library, Research Briefing n° CBP-10935, 2 juillet 2026, disponible sur : <https://commonslibrary.parliament.uk>.

96. Voir par exemple M. A. Milley et E. Schmidt, « America Isn't Ready for the Wars of the Future. And They're Already Here », *Foreign Affairs*, 5 août 2024.

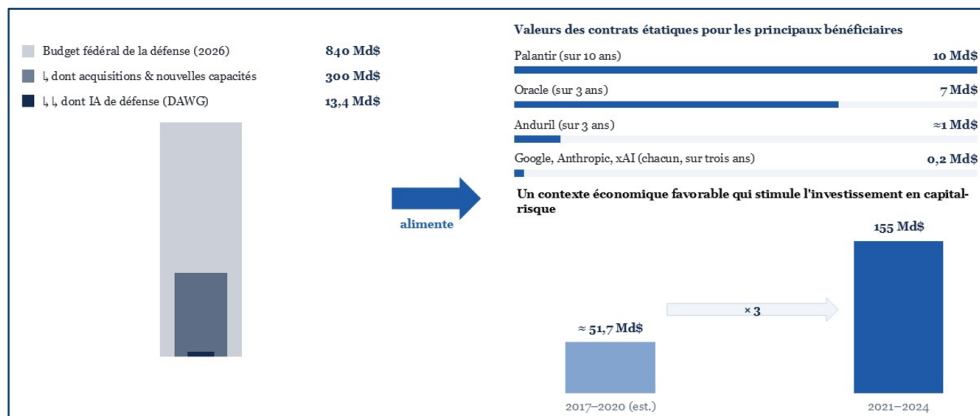
97. Ces contrats ont été passés très majoritairement auprès du Pentagone et, dans une moindre mesure, auprès des agences de renseignement. Voir *Digital Destroyers: How Big Tech Sells War on Our Communities*, 2021, disponible sur : <https://bigtechsellswar.com>.

98. Le montant annuel de leurs contrats avec le Pentagone est passé de 50 millions de dollars en 2010 à 400 millions en 2020 et a atteint près de 650 millions en 2024. Pour un détail des contrats d'Amazon, Google, Microsoft et Oracle, Voir A. Coveri *et al.*, « Big Tech and the US Digital-Military-Industrial Complex », *op. cit.*

99. L. Mediavilla, « Le champ de bataille évolue aussi vite que la technologie que vous avez dans votre poche : pourquoi le Pentagone s'allie à la Silicon Valley », *Le Figaro*, 30 novembre 2025 ; « US Defense Department Awards Contracts to Google, Musk's xAI », *op. cit.* ; J. Novet, « Oracle Signs 10-Year Software Contract with Pentagon Worth up to \$7 Billion », *CNBC*, 23 juillet 2026.

100. Z. Corbyn, « Move Fast, Kill Things: The Tech Startups Trying to Reinvent Defence with Silicon Valley Values », *The Guardian*, 29 mars 2025.

Illustration 1 : La demande publique augmente et profite à la *tech*



Sources : J. Isler, « DOD AI Initiatives Will Open the Door to New Opportunities », *Washington Technology*, 22 août 2025 ; « Defense Tech Trends 2026 », disponible sur : www.clipperdefense.com ; A. Down, « Pentagon Asks for 54\$bn in Pivot Towards AI-powered War », *The Guardian*, 22 avril 2026 ; L. Mediaville, « Le champ de bataille évolue aussi vite que la technologie que vous avez dans votre poche : pourquoi le Pentagone s'allie à la Silicon Valley », *Le Figaro*, 30 novembre 2026 ; « US Defense Department Awards Contracts to Google, Musk's xAI », op. cit. ; J. Novet, « Oracle Signs 10-Year Software Contract with Pentagon Worth up to \$7 Billion », *CNBC*, 23 juillet 2026.

Le capital-risque sous la bannière de l'*American Dynamism*

À l'heure de la financiarisation généralisée des économies et de la marchandisation néolibérale du secteur de la défense, le capital-risque américain joue de fait un rôle majeur dans la militarisation de la *tech*, en stimulant fortement la croissance de la *DefTech*. Les fonds impliqués sont légion¹⁰¹, et leurs investissements et prises de participation sont en très forte hausse sur les dernières années. Entre 2020 et 2023, près de 125 milliards de dollars issus du capital-risque ont ainsi été injectés dans des entreprises de *DefTech*, contre 43 milliards entre 2016 et 2020¹⁰². Au seul troisième trimestre de l'année 2025, ce montant atteignait près de 40 milliards de dollars¹⁰³. Cette dynamique est également observable en Europe, où le nombre de fonds spécialisés a très fortement progressé au cours des dernières années¹⁰⁴ et où Munich semble s'imposer comme le cœur de l'écosystème¹⁰⁵.

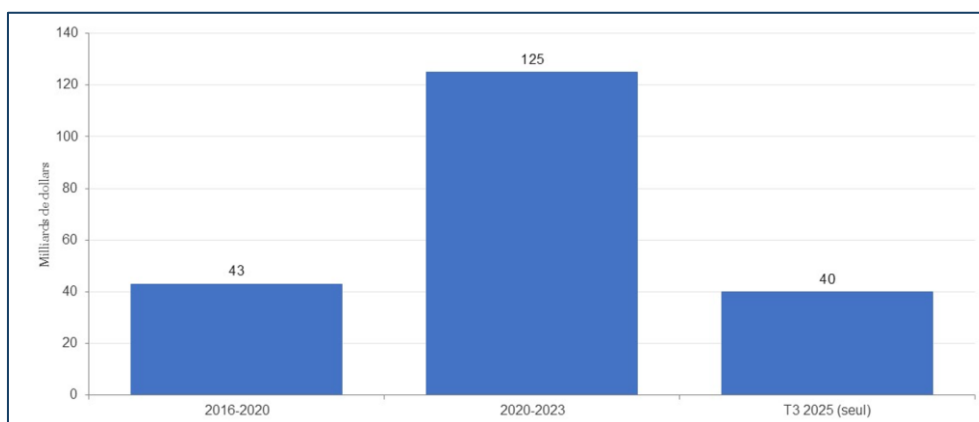
101. Pour une liste non exhaustive : A16z (Andreessen Horowitz) ; Founders Fund (Peter Thiel) ; Sequoia Capital ; Vision Fund (SoftBank) ; Accel Partners ; General Catalyst ; Lightspeed ; Shield Capital ; Khosla Ventures ; Lux Capital ; Prosus Ventures ; Veritas Capital ; Paladin Capital ; Arlington Capital Partners ; Behrman Capital. Voir J. M. Predin, « VCs Fuel the Boom in Defense and Military Startups Amid Global Conflicts », *Forbes*, 2 novembre 2023.

102. E. Lipton, « New Spin on a Revolving Door », op. cit.

103. PitchBook, *Q3 2025 Defense Tech VC Trends*, 2025, disponible sur : <https://pitchbook.com>.

104. Entre 2024 et 2025, neuf nouveaux fonds spécialisés ont été créés, pour un total dépassant la trentaine dans l'Europe entière. Pour une liste non exhaustive à la mi-2025, voir « Les fonds d'investissement de Defense Tech en Europe », *FrenchWeb*, 7 juillet 2025.

105. P. Sautreuil, « Drones, IA, robots... Munich se rêve en capitale européenne de la "Défense Tech" », *La Croix*, 15 mars 2026.

Illustration 2 : Le boom des investissements en DefTech

Sources : E. Lipton, « *New Spin on a Revolving Door* », op. cit. ; PitchBook, *Q3 2025 Defense Tech VC Trends*, 2025.

Légende : Capital-risque injecté dans les entreprises de défense technologique (en Md\$).

Alors que les perspectives de retour rapide sur investissement s'amenuisent dans les autres secteurs industriels, les capital-risqueurs n'ont pas manqué de saisir ce qu'ils ont perçu comme une opportunité¹⁰⁶. Bien introduits auprès des cercles décisionnels, ces acteurs contribuent directement à attirer d'anciens hauts responsables du Pentagone dans les rangs des startups, et donc plus largement à remodeler le paysage de la défense¹⁰⁷. Plusieurs d'entre eux, à l'image de l'icône du capital-risque M. Andreessen et son *American Dynamism*¹⁰⁸, ont ainsi lancé une série d'initiatives de « capital patriotique¹⁰⁹ », ce qui en fait des acteurs non plus seulement financiers mais aussi politiques, capables d'imposer des changements de vision et donc de culture stratégique du Pentagone. Cette

106. « Le capital est tellement concentré qu'il doit rechercher des opportunités d'investissement viables, en raison à la fois de la nécessité de sa valorisation et de la baisse des investissements publics dans les secteurs non militarisés, tels que les infrastructures et les programmes sociaux. Dans ces conditions, le complexe militaro-industriel devient un secteur cible privilégié pour les gestionnaires d'actifs et d'autres acteurs de la finance privée ». Voir S. Marshall, « A Violent Convergence: How Silicon Valley and Private Finance Are Reshaping War », *Security in Context*, 16 avril 2026, disponible sur : www.securityincontext.org.

107. E. Schwarz, « The Silicon Valley Venture Capitalists Who Want to "Move Fast and Break Things" in the Defence Industry », *The Conversation*, 16 janvier 2025.

108. Conceptualisé début 2022 par Katherine Boyle, associée-fondatrice du fonds de capital-risque a16z, l'*American Dynamism* entend 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.

109. Tels le Special Competitive Studies Project d'Eric Schmidt (www.scsp.ai) ; Rebooting the Arsenal of Democracy de Palmer Luckey (www.rebootingthe arsenal.com) ; l'America's Frontier Fund initié par Peter Thiel et Eric Schmidt (www.americasfrontier.com) ; le 8VC Build Program de Joe Lonsdale, co-fondateur de Palantir (8vc.com) ; US Innovative Technology de Thomas Tull (www.usitfund.com) ; la Security and Resiliency Initiative de JP Morgan Chase (www.jpmorgan.com) ; le Deterrence Fund de Point72 (point72.com) ; l'US Strategic Tech Fund d'Alumni Ventures (www.av.vc) ; Lux Ventures IX de Lux Capital (www.luxcapital.com).

logique a trouvé son aboutissement en mars 2025 avec la nomination au poste de secrétaire adjoint à la Guerre de Stephen Feinberg, co-fondateur et directeur général de la société de gestion de fonds d'investissement Cerberus Capital Management¹¹⁰.

Les capital-risqueurs se retrouvent dès lors en position d'imposer leur vision, leur temporalité et leurs intérêts, qui recoupent très largement ceux des startups et leur « logique produit » et « *software first* »¹¹¹. Une vision dans laquelle l'État doit s'effacer au profit d'un pan du secteur privé jugé plus efficace et où le produit fini compte moins que le produit d'appel pour obtenir des contrats publics. Ceux-ci valent reconnaissance de ce qui ne demeure qu'un simple potentiel, mais suffisent néanmoins à entraîner une valorisation exponentielle de l'entreprise, et donc à préparer une sortie de capital fructueuse. Une telle dynamique de financiarisation alimente en retour une bulle spéculative susceptible de fragiliser à terme l'ensemble de l'écosystème¹¹². Car la croissance capitaliste rapide est le seul produit que les fonds vendent à leurs clients, bien davantage qu'une technologie effective. Dès lors, loin des planifications et processus contractuels pluriannuels de l'administration militaire, l'horizon des capital-risqueurs est celui des cycles de *hype* court-termistes, qui nécessite d'aller vite – dans la plus pure tradition de la devise de Facebook (« *Move fast and break things* ») – et d'œuvrer à la dérégulation du secteur afin de lever les contraintes réglementaires et les obligations de mise en conformité¹¹³.

Cette vision et ces mantras sont assumés et répétés à l'envi au sein des Livres blancs, manifestes et autres textes aux accents programmatiques qui sont produits en nombre par de tels acteurs, sous couvert de patriotisme¹¹⁴. Des récits prennent ainsi corps pour imposer au monde militaire une alliance avec les investisseurs, les ingénieurs et dirigeants de la *tech*, afin d'endiguer un prétendu déclin national et protéger les États-Unis et la « civilisation occidentale » qui seraient menacés de disparition¹¹⁵.

110. « Steve Feinberg », biographie officielle, Département de la Guerre, disponible sur : www.war.gov.

111. E. Schwarz, « When War Becomes a Tech Product: How Silicon Valley Logics Are Reshaping Military AI », *Untold Mag*, 22 juin 2025.

112. S. Munger, « Startupisation militaire : la guerre sous influence de la Silicon Valley », *Le Rubicon*, 29 mai 2026 ; A. Parker, « Thanks to Drones, China and Ukraine, a Record Number of Military Startups Became Unicorns in 2025 », *Forbes*, 28 novembre 2025.

113. E. Schwarz, « From Blitzkrieg to Blitzscaling: Assessing the Impact of Venture Capital Dynamics on Military Norms », *Finance and Society*, 2025, p. 1-24.

114. Le plus iconique est sans doute celui produit par Palmer Luckey (www.anduril.com), mais il en existe de nombreux autres, à l'image de celui du fonds A16z (a16z.com) ou de General Catalyst (www.generalcatalyst.com).

115. S. Marshall, « A Violent Convergence », *op. cit.* Ce déclin remonterait, selon leurs récits, au « Last Supper », en référence à un dîner de l'été 1993 lors duquel l'administration Clinton avait signifié à l'industrie de la défense que les budgets fédéraux allaient se réduire avec la fin de la guerre froide, entraînant privatisation, contraction et restructuration de l'ensemble du secteur. Mais en réalité, la dérégulation et la financiarisation introduites par le néolibéralisme reaganien avaient déjà amorcé la lente désagrégation de cette filière stratégique. Voir M. Mullins, « What Silicon Valley Gets Wrong About National Security: Defense Tech Innovation Requires Government Intervention », *Foreign Affairs*, 8 janvier 2026.

L'hypothèse d'un « *backlash* »

Il existe une dernière lecture de ce virage militaire de la *tech*. Celle-ci l'interprète moins comme une réponse au contexte géopolitique et économique que comme le contrecoup d'une décennie au cours de laquelle l'industrie technologique aurait été dominée par les valeurs progressistes de ses salariés. Dans ce récit, popularisé par les figures de la droite néoréactionnaire, la période des pétitions et des chartes éthiques aurait constitué une parenthèse idéologique imposée aux dirigeants par une génération d'employés militants, qu'il s'agirait aujourd'hui de refermer.

Marc Andreessen, l'un des investisseurs les plus influents de la Silicon Valley, en a donné l'interprétation la plus articulée. À l'en croire, c'est la radicalisation progressiste des jeunes diplômés entrés dans l'industrie à partir de 2013, puis la prétendue percée *woke* qui s'est ensuivie, qui auraient rompu le pacte tacite unissant la *tech* au Parti démocrate et jeté ses élites dans les bras de Donald Trump¹¹⁶. Le retour en grâce des applications militaires participe, selon cette grille de lecture, du retour à une virilité entrepreneuriale décomplexée, dont Mark Zuckerberg s'est fait le héraut en appelant à réinjecter de l'« énergie masculine » dans des entreprises jugées « émasculées¹¹⁷ ». Le virage militaire serait ainsi la pointe avancée d'un « *backlash* », un retour de bâton après que le progressisme est allé « trop loin ».

À cela s'ajoutent les griefs exprimés contre une décennie d'efforts réglementaires envers le secteur, venus des démocrates. La présidence Biden a de fait rompu avec les années Obama, en confiant la Federal Trade Commission à Lina Khan et la division *antitrust* du ministère de la Justice à Jonathan Kanter, dont les nominations se sont traduites par des poursuites contre Google, Amazon, Apple et Meta. Dans le même temps, la Securities and Exchange Commission s'est engagée dans une politique répressive à l'égard des cryptoactifs ; tandis que Joe Biden signait en octobre 2023 son fameux décret sur l'IA, qui imposait des obligations de transparence aux développeurs de modèles de pointe. Les efforts de réglementation de la *tech* sont alors vus comme le prolongement institutionnel du militantisme des salariés.

Cette lecture éclaire la dimension idéologique du tournant pris par les élites technologiques aux États-Unis. Celui-ci pourrait toutefois se révéler risqué pour ses promoteurs, en particulier si l'opinion, les talents et les clients prennent leurs distances avec ce discours. Plusieurs signaux récents suggèrent en effet que la tendance pourrait à nouveau s'inverser et que

116. « How Democrats Drove Silicon Valley into Trump's Arms », entretien de Marc Andreessen avec Ross Douthat, *The New York Times*, 17 janvier 2025 ; N. Smyrniotis, « Understanding Silicon Valley's Reactionary Turn », *La Pensée*, n° 423, 2025.

117. Propos tenus par Mark Zuckerberg dans le podcast de Joe Rogan, janvier 2025 ; A. Marcotte, « The Tech Billionaire War on "Woke" Is Really Targeting Workers », *Salon*, 17 janvier 2025.

l'alignement inconditionnel sur la puissance d'État pourrait se retourner contre ceux qui le défendent.

Le premier signal est venu du marché lui-même, à la faveur du bras de fer entre Anthropic et le Pentagone¹¹⁸. En refusant de lever ses lignes rouges, l'entreprise a renoncé à un contrat de 200 millions de dollars et s'est exposée aux représailles de l'administration. Pourtant, loin de la fragiliser, ce refus pourrait s'avérer, selon la formule d'un observateur, « le meilleur investissement marketing de la Silicon Valley depuis des années¹¹⁹ ». En effet, alors qu'il était annoncé le 1^{er} mars 2026 que le rival d'Anthropic, OpenAI, avait récupéré le contrat, les téléchargements de l'application Claude ont bondi de près de 70 % en une journée¹²⁰.

Un autre signal touche à la ressource la plus disputée de l'industrie que sont les talents. Le 15 juillet 2026, Alex Turner, chercheur en sûreté de l'IA chez Google DeepMind, a rendu publiques sur X les raisons de sa démission, intervenue quelques semaines plus tôt. L'entreprise aurait « rompu sa promesse fondatrice » en collaborant avec l'armée sans restriction contre les armes autonomes ni la surveillance de masse¹²¹. Son récit, largement relayé, documente de l'intérieur des mois d'efforts infructueux pour faire tenir à Google ses engagements éthiques, jusqu'au constat désabusé que « les promesses de conscience se volatilisent souvent au contact du pouvoir¹²² ». Or, dans une industrie où la guerre des talents fait rage et où les chercheurs de premier plan ont l'embarras du choix, chaque départ publicisé pour des raisons de conscience profite aux entreprises proposant une alternative.

Rien ne garantit, à ce stade, que ces signaux annoncent un retournement d'ampleur. Le rapport de force politique et budgétaire demeure favorable aux convertis du techno-patriotisme, et l'histoire récente invite à envisager avec prudence la capacité d'ingénieurs mobilisés à infléchir durablement les stratégies d'entreprise. En revanche, ces deux cas rappellent que les entreprises de la *tech*, dans leurs orientations idéologiques, ne peuvent ignorer complètement l'opinion des utilisateurs ni la conscience des salariés.

118. Ce cas illustre par la même occasion la volonté de l'administration Trump d'utiliser toute une panoplie d'outils — créés pour l'occasion ou issus d'une interprétation juridique originale — pour contraindre les entreprises à s'aligner sur son programme politique et faire taire ses critiques.

119. K. Scanlon, « In Graphic Detail: How Anthropic's Pentagon Refusal Is Paying off in Downloads, Brand Trust and Enterprise Deals », Digiday, 9 mars 2026.

120. *Ibid.*

121. H. Langley, « A DeepMind Researcher Resigned over Its AI Military Deal », *Business Insider*, 15 juillet 2026.

122. A. Turner, « Why I Left Google DeepMind », Turntrout, 15 juillet 2026, disponible sur : turntrout.com.

Vers une privatisation de la défense ?

En février 2022, alors que la Russie était en train d'envahir le pays, Elon Musk activait Starlink au-dessus de l'Ukraine à la demande des autorités ukrainiennes, leur rendant ainsi la capacité de commandement que leur infrastructure publique ne leur assurait plus¹²³. La décision de cet entrepreneur privé, saluée sur le moment, aurait en réalité dû alerter. Quelques mois plus tard en effet, le même Elon Musk refusait d'étendre la couverture de ses satellites au-dessus de la Crimée afin d'empêcher une opération militaire ukrainienne, s'arrogeant de fait un droit de veto sur la conduite de la guerre. Alors, quand les capacités critiques de la défense reposent sur des infrastructures privées, qui, de l'État ou de l'entreprise, exerce en dernier ressort la souveraineté ?

Un empiètement sur les fonctions régaliennes

En plus d'acter la marchandisation du service public le plus stratégique qui soit, l'empiètement croissant de la *tech* sur le champ militaire induit un certain nombre de risques pour les appareils étatiques¹²⁴. Car le secteur de la défense n'est pas un marché classique mais s'avère profondément biaisé (à forte consommation de capital, motivé par un acheteur unique, en fonction de contextes politiques et géopolitiques volatils), et réclame prévisibilité et lisibilité. Le premier risque est donc de voir les capacités et l'expertise structurelles s'amenuiser durablement, alors que celles-ci demeurent indispensables à toute planification stratégique. La délégation mal maîtrisée de compétences peut ainsi provoquer des erreurs sur les plans tactique comme stratégique. L'illustration a pu en être donnée récemment lors de l'opération *Epic Fury* menée par Washington contre l'Iran, lors de laquelle la délégation partielle de la planification à Palantir a conduit les États-Unis à commettre des crimes de guerre¹²⁵.

123. W. Isaacson, *Elon Musk*, New York, Simon & Schuster, 2023.

124. Cette marchandisation vaut également pour le champ cyber, dans lequel l'administration Trump semble déléguer une partie de ses prérogatives au secteur privé pour lutter contre les « organisations criminelles transnationales ». Voir N. Robins-Early, « Donald Trump Empowers US Private Companies to Conduct Cyber-Attacks », *The Guardian*, 13 août 2026.

125. K. T. Baker, « AI Got the Blame for the Iran School Bombing. The Truth Is Far More Worrying », *The Guardian*, 26 mars 2026.

Une relation de dépendance technique se noue également, dans la mesure où les entreprises ne sont pas uniquement les fournisseurs mais également les gestionnaires d'équipements dont elles sont les seules à pouvoir assurer le maintien en condition opérationnelle (*via* des mises à jour, reprogrammations, itérations...). Si cette relation de dépendance préexistait aux liens unissant États et BITD traditionnelle, la différence réside ici dans le fait que les entreprises de la *DefTech* ne répondent pas à des commandes mais imposent leurs produits sur étagère et contractent par ailleurs avec davantage de partenaires que les seuls gouvernements. En outre, à mesure que la valeur des armements se déplace du matériel vers le logiciel et que le savoir proprement militaire doit composer toujours davantage avec un savoir technique, le déficit d'expertise interne aux armées et la complexité croissante des équipements accroissent très largement le niveau de dépendance – comme l'a une fois encore rappelé l'affaire Anthropic. La fiabilité des solutions proposées étant par ailleurs loin d'être garantie, la puissance publique peut se retrouver à devoir assumer des risques dont elle n'a pas la maîtrise, en particulier dans le champ cyber¹²⁶.

La dépendance étatique à des acteurs non étatiques soulève dès lors d'évidents enjeux de souveraineté. La défense prend le risque de se voir vampirisée par certains acteurs privés qui auront un intérêt économique à l'extension temporelle et géographique de la guerre. Et ce d'autant plus que ces entreprises doivent *in fine* rendre des comptes à leurs investisseurs en quête de profits et sont donc moins susceptibles de répondre uniquement aux divers besoins et attentes des administrations régaliennes. La culture du risque et du bouleversement de l'ordre établi, importée depuis l'univers du capital-risque et des startups, ne peut que renforcer cette préoccupation. Par ailleurs – comme l'Ukraine a pu amèrement en faire l'expérience –, la fiabilité politico-morale de certains partenaires peut constituer un enjeu majeur pour les États concernés, soumis aux éventuels revirements de leurs fournisseurs. À l'heure où certaines figures de la *tech* revendiquent un positionnement ou des responsabilités politiques de plus en plus affirmés, elle représente un défi tout particulier aux États-Unis. L'affaire Anthropic a ainsi incité le Pentagone à multiplier les partenariats (avec xAi, Google et OpenAI) et les discussions (avec Microsoft, Amazon, NVIDIA et Reflection AI), afin d'échapper à tout enfermement propriétaire (« *vendor lock-in*¹²⁷ »). Les logiques de vassalisation dans un sens ou dans l'autre jouent ici à plein et offrent la traduction simultanée du rapport de force opposant la puissance publique à ses contractants.

126. « Anduril and Palantir Battlefield Communication System “Very High Risk,” US Army Memo Says », CNBC, 3 octobre 2025 ; H. Khlaaf et S. Myers West, « The Rush to A.I. Threatens National Security », *The New York Times*, 27 janvier 2025.

127. J. E. Barnes et S. Frenkel, « Pentagon Makes Deals with A.I. Companies to Expand Classified Work », *The New York Times*, 1^{er} mai 2026.

À l'inverse des précédents, le dernier écueil concerne cette fois-ci les entreprises et réside dans l'amalgame inhérent à une telle collusion public-privé. Celle-ci est susceptible de mettre les acteurs technologiques à la merci de décisions en haut lieu sur de grands projets stratégiques à la nécessité douteuse, à l'image de « La Guerre des étoiles » promue par Ronald Reagan, ou encore de l'invasion russe de l'Ukraine déclenchée par Vladimir Poutine. Plus encore, cette imbrication expose également les entreprises en les désignant comme des cibles potentielles et pour partie légitimes aux yeux d'adversaires stratégiques. Ceci est valable sur les plans cyber et cinétique, comme l'ont montré les frappes de l'Iran contre les infrastructures d'Amazon aux Émirats arabes unis et à Bahreïn, ainsi que les menaces proférées contre celles d'OpenAI dans la région¹²⁸. Le principe de distinction propre au droit international humanitaire (DIH) s'efface dès lors au profit d'un amalgame porteur de dérives.

La matrice de bascules autoritaires

La privatisation de la défense engendre également des préoccupations d'ordre démocratique et citoyen. En premier lieu, elle accélère la bascule des usages du domaine militaire vers la sphère civile, encourageant plus ou moins directement le recours à des technologies de surveillance, de ciblage et de contrôle potentiellement désastreuses pour la préservation des droits humains¹²⁹. Si ces pratiques sont déjà bien documentées dans les régimes autoritaires, elles se sont aussi invitées au cœur des démocraties occidentales à compter de 2001. Les campagnes de traque, d'enfermement et d'expulsion des populations migrantes ou immigrées menées par l'Immigration and Customs Enforcement (ICE) américaine l'ont ainsi abondamment rappelé au cours des dernières années¹³⁰. Or, l'absence de contrôle démocratique sur le déploiement de technologies sécuritaires encourage, de fait, les pratiques abusives et les déagements de responsabilité qui abîment la paix civile. Les multiples tentatives – y compris en France – d'inscrire ces usages techno-sécuritaires dans le droit, réalisées sans aval ni consultation des citoyens élargis, risquent dès lors d'attiser des tensions déjà fortes¹³¹.

Le « *backlash* » et les manifestes évoqués plus haut ne laissent par ailleurs aucun doute sur la volonté d'un certain nombre de leaders technologiques américains d'œuvrer à une lutte contre des ennemis désignés, aussi bien à l'intérieur qu'à l'extérieur : leur soutien logistique, technique,

128. J. Hsu, « Iran Struck Amazon Data Centers Again amid Widening War, Satellites Show », *Ars Technica*, 30 juillet 2026.

129. Comme le note le chercheur Félix Tréguer, « on peut s'attendre à ce que tout un tas de gadgets policiers soient financés avec l'argent associé au réarmement de la France et de l'Europe », cité dans S. Kloetzli, « Comment la guerre profite aux géants de l'IA », *Usbek & Rica*, 8 juillet 2025.

130. « Fabrice Leggeri jugé pour complicité de crimes contre l'humanité : Frontex, l'ICE des Européens ? », *Courrier international*, 25 mars 2026 ; J. Cox, « Leaked Document Shows the Surveillance Tech at ICE's Fingertips », *404 Media*, 23 juillet 2026.

131. T. C. Jusquiamé, « Vidéosurveillance "intelligente" : bientôt une loi taillée sur mesure pour les intérêts privés ? », *Observatoire des multinationales*, 26 mai 2026, disponible sur : www.multinationales.org.

voire politique aux actions menées par l'ICE et la Customs Border Protection (CBP) en atteste très largement¹³². Leur niveau d'influence politico-économique représente un double sujet de préoccupation. Premièrement sur le plan démocratique, en raison du poids démesuré qu'ils exercent aussi bien sur les cycles électoraux que sur la gouvernance de l'administration Trump II¹³³. Mais aussi sur le plan stratégique, dans la mesure où nombre d'entre eux souhaitent imposer leurs vues techno-solutionnistes sans bien souvent entendre quoi que ce soit à la chose militaire¹³⁴.

Ensuite, dans la mesure où ces acteurs technologiques sont devenus les yeux et les oreilles de divers gouvernements tant sur les plans intérieur qu'extérieur, ils se retrouvent en position d'accéder à des informations sensibles et donc à un pouvoir qui leur donnent un ascendant vis-à-vis de ces mêmes États – ascendant dont ils n'hésitent pas à user pour servir leurs intérêts¹³⁵. En accroissant la dépendance structurelle à leurs infrastructures, ces entreprises renforcent de fait leur pouvoir de négociation vis-à-vis de ceux qui sont aussi leurs régulateurs : perçues comme des actifs stratégiques, elles peuvent espérer un traitement plus favorable sur d'autres dossiers aux forts impacts démocratiques (fiscalité, accompagnement financier, concurrence, responsabilité juridique, etc.). Là encore, la différence de degré avec l'influence exercée par les entreprises de la BITD traditionnelle tient au fait que les acteurs de la *tech* déploient leurs activités de manière horizontale et ont donc des intérêts qui vont bien au-delà des seuls secteurs de la défense ou du renseignement.

Enfin, il faut garder à l'esprit que les montants alloués au développement techno-militaire et techno-sécuritaire détournent aussi ces financements d'autres priorités tout aussi stratégiques, y compris dans le même champ d'action – qu'on songe à la reconstitution de stocks militaires, au maintien en condition opérationnelle des équipements, ou à la diplomatie par exemple. La quête de rentabilité peut aussi contribuer à détacher durablement des capital-risqueurs et des startups d'autres secteurs non moins essentiels – tels la santé ou le climat – sur lesquels ils s'étaient pourtant préalablement investis¹³⁶. Cette logique de fond n'est toutefois pas

132. C. Haskins, « All the Ways Big Tech Fuels ICE and CBP », *Wired*, 3 mars 2026.

133. W. D. Hartung, « At this Point, Silicon Valley Militarists Aren't Just Greedy — They're Bloodthirsty », *The Nation*, 21 mars 2025.

134. Palmer Luckey reconnaît lui-même avoir embauché « plus de lobbyistes et d'avocats que d'ingénieurs » pour promouvoir son modèle d'affaires auprès des cercles décisionnels et redéfinir les exigences et prérequis des programmes d'armement en fonction de la technologie produite par son entreprise. Voir « Palmer Luckey and Anduril Want to Shake up Armsmaking », *The Economist*, 20 juin 2024.

135. À titre d'exemple, Palantir et SpaceX n'ont pas hésité à poursuivre en justice l'administration américaine pour accéder à des appels d'offres, décrochant ensuite des missions clés dans la gestion des données militaires. Elles ont ainsi créé un précédent, et ce genre de manœuvre s'est depuis répété. Voir A. Coveri et al., « Blurring Boundaries: An Analysis of the Digital Platforms-Military Nexus », *Review of Political Economy*, vol. 37, n° 4, 2024, p. 1632-1663.

136. Cette logique a cours aux États-Unis, où des startups initialement investies dans la lutte contre le réchauffement climatique (Magrathea Metals, Brimstone, VEIR) ont depuis réorienté leurs activités vers la sécurité nationale. Mais l'Europe n'est pas épargnée : le fondateur d'Helsing concentrait à l'origine ses efforts sur l'analyse d'images médicales avant d'être approché par le secteur militaire. Voir E. Ballard,

propre au seul champ techno-militaire : le cas le plus emblématique est sans doute le récent démantèlement par Google de l'équipe de développement d'Alpha Fold – le programme d'IA ayant permis des avancées majeures dans la recherche biomoléculaire, récompensées par un prix Nobel¹³⁷.

Des résistances encore modestes

L'appétence des *Big Tech* pour la signature de contrats avec le Pentagone au cours de la dernière décennie ne s'est toutefois pas imposée sans heurts, et des actes de résistance lui ont été opposés. Ceux-ci ont pu prendre diverses formes en fonction des contextes et des entreprises : pétitions internes, manifestes et lettres ouvertes signés par des salariés, démissions collectives ou individuelles, voire véritables mobilisations syndicales – ce qui demeure rare dans un secteur traditionnellement éloigné de toute culture et donc structuration syndicales.

Divers contrats se sont ainsi vus contester au cours des dernières années, avec plus ou moins de succès. Le recul de Google sur le projet Maven – passé depuis chez Palantir – après une mobilisation massive de ses salariés en 2018 demeure le plus spectaculaire et porteur. Quelques semaines plus tard, des employés de Salesforce, Amazon et Microsoft avaient ainsi annoncé la fin des contrats liant leurs entreprises aux agences chargées du contrôle migratoire (ICE et CBP), après des révélations sur les séparations de familles opérées à la frontière mexicaine¹³⁸. Début 2019, une centaine d'employés de Microsoft avaient également protesté contre un contrat à 480 millions de dollars pour fournir à l'armée américaine des casques de réalité augmentée¹³⁹.

Ces cas d'école n'ont toutefois ouvert qu'une brèche temporaire au sein de ces entreprises, et joué un rôle d'épouvantail pour l'ensemble du secteur. Ce dernier s'est depuis appliqué à mieux dissimuler ses partenariats sensibles et à étouffer les dissensions en amont. D'autres contestations internes à Google, telle celle menée autour du projet Nimbus (offre de *cloud* pour l'armée israélienne en partenariat avec Amazon), ont ainsi entraîné le licenciement d'employés¹⁴⁰. Des manœuvres similaires ont eu lieu chez Cisco et Microsoft après des mobilisations contre la signature des contrats JEDI (abandonné à la suite d'un contentieux avec Amazon), HoloLens ou pour dénoncer la fourniture d'IA à Israël (« *No Azure for Apartheid* »), tandis qu'Amazon, Salesforce ou Clarifai ont simplement ignoré les protestations en

« Startups That Set out to Fix the Climate Are Now Talking About Jet Fighters », *The Wall Street Journal*, 23 mars 2025 ; Y. Khan, « Venture Capitalists Likely to Continue Pivoting Away from Climate in 2026 », *The Wall Street Journal*, 30 décembre 2025.

137. « Google DeepMind Dismantles Nobel-Winning AlphaFold Team in Strategy Shift », *Financial Times*, 29 juillet 2026.

138. R. Sandler, « Amazon, Microsoft, Wayfair: Employees Stage Internal Protests Against Working with ICE », *Forbes*, 29 juillet 2019.

139. Le contrat IVAS (Integrated Visual Augmentation System) prévoyait des casques destinés à « accroître la létalité » du combattant.

140. « No Tech for Apartheid. Google licencie 28 employés qui protestaient contre un contrat d'IA avec Israël », *Courrier international*, 18 avril 2024.

leur sein¹⁴¹. Le raidissement des *Big Tech* face aux lanceurs d'alerte et à toute tentative de remise en cause interne est ainsi manifeste et laisse jusqu'ici peu de place à l'émergence d'un potentiel front uni des travailleurs de la *tech*¹⁴².

Quand bien même le syndicalisme reste encore trop timoré au sein de ces entreprises pour imposer un rapport de force durable face aux diverses stratégies d'obstruction qui lui sont opposées¹⁴³, la contestation persiste et se structure autour de modestes mouvements internes ou externes à ces entreprises, à partir de préoccupations politiques nationales comme internationales¹⁴⁴. À la suite de révélations médiatiques, certaines pressions ont pu aboutir à des inflexions, à l'image de la rupture partielle du contrat qui liait Microsoft à l'unité 8 200 de l'armée israélienne (impliquée dans l'espionnage et la surveillance de masse des Palestiniens) et du limogeage du directeur général de Microsoft Israel¹⁴⁵. Par ailleurs, les abus de l'ICE – qui ne cache pas son goût pour les technologies duales produites par la Silicon Valley – et, plus encore, « l'affaire Anthropic » pourraient bien redonner un second souffle à ces protestations¹⁴⁶.

Des salariés de Google et d'OpenAI ont ainsi pu exprimer leur solidarité avec Anthropic¹⁴⁷, tandis que, tout récemment, 600 salariés de Google ont signé une nouvelle lettre ouverte demandant à leur direction de renoncer à fournir des modèles d'IA au Pentagone pour mener des opérations classifiées sans garanties préalables¹⁴⁸. Alors qu'OpenAI s'est positionné pour remplacer Anthropic auprès du Pentagone, la pression exercée sur Sam Altman l'a incité à reconnaître le caractère opportuniste de sa démarche et à annoncer la renégociation du contrat pour en exclure les usages à des fins de surveillance nationale.

141. D. Gibson, « The Effectiveness of Employee Activism in Big Tech-DoD Partnerships », *The Pardee Atlas Journal of Global Affairs*, 2024.

142. N. Nix *et al.*, « Big Tech Takes a Harder Line Against Worker Activism, Political Dissent », *The Washington Post*, 16 mai 2025.

143. Voir par exemple M. Mermoz, « Amazon accusé de toutes parts de se livrer à de la répression syndicale », *Mediapart*, 19 février 2026 ; M. Coulter, « Google Has Been Ordered to Unseal Dozens of Documents Related to Its Secret Anti-Union Campaign "Project Vivian" », *Business Insider*, 1^{er} décembre 2021.

144. Tels « No Tech for Apartheid », coalition d'employés de la *tech* contre l'implication de leurs entreprises dans le génocide des Palestiniens, ou « Purge Palantir », groupe de militants externes engagés contre la firme et ses agissements.

145. Microsoft n'a pas pour autant rompu l'ensemble de ses liens contractuels avec l'armée israélienne. Voir H. Davies et Y. Abraham, « Microsoft Blocks Israel's Use of Its Technology in Mass Surveillance of Palestinians », *The Guardian*, 25 septembre 2025.

146. Dans une lettre ouverte à leurs dirigeants, près d'un millier de salariés de Google se sont insurgés contre les liens unissant l'entreprise à l'ICE et à la CBP. Voir L. Neelakandan, « Nearly a Thousand Google Workers Sign Letter Urging Company to Divest from ICE, CBP », *CNBC*, 26 mars 2026. Amazon, Google, Microsoft et OpenAI ont aussi été appelés par une coalition de syndicats à s'aligner sur les lignes rouges édictées par Anthropic. Voir M. Day et K. Manson, « Anthropic Sees Support from Other Tech Workers in Feud with Pentagon », *Bloomberg*, 27 février 2026.

147. H. Gold, « Some OpenAI Staff Are Fuming About Its Pentagon Deal », *CNN*, 4 mars 2026 ; T. Mikke, « Google Workers Seek "Red Lines" on Military A.I., Echoing Anthropic », *The New York Times*, 26 février 2026.

148. « IA : plus de 600 salariés de Google demandent à leur direction de ne pas fournir des modèles à l'armée américaine », *Le Monde*, 28 avril 2026.

Dans ce contexte, l'issue de la bataille juridique entre Anthropic et le DoD sera donc scrutée de près par l'ensemble des acteurs, comme traduction d'un rapport de force plus large à l'œuvre dans la Silicon Valley autour des enjeux éthiques. Et ce d'autant plus qu'à l'heure où l'IA pèse directement sur l'employabilité des cols blancs nouvellement précarisés, les contestations des travailleurs du secteur refont surface (notamment chez Meta, Google, Oracle) et pourraient se multiplier dans les mois à venir, dans les pas de mouvements tels que « *Stop the AI Race* » ou « *Pause AI* »¹⁴⁹. L'opposition croissante à l'implantation de centres de données, qui constitue déjà un enjeu politique aux États-Unis, pourrait bientôt s'étendre à l'Europe et alimenter cette dynamique¹⁵⁰. Si la convergence des luttes semble encore lointaine, elle pourrait toutefois être encouragée par l'inflexibilité des élites dirigeantes face aux revendications. En ce sens, la syndicalisation en hausse peut être lue comme les prémices d'une possible évolution du rapport de force¹⁵¹.

Une Europe enfermée dans une dépendance structurelle ?

Le paysage européen de la *DefTech* pourrait laisser penser qu'une souveraineté technologique européenne dans le domaine militaire est en train de voir le jour, comme en attestent les 8,7 milliards de dollars de levée de fonds pour l'année 2025, en croissance de 55 %¹⁵². Ce serait toutefois confondre l'émergence d'acteurs européens avec la construction d'une véritable autonomie stratégique. En effet, ces champions, pour prometteurs qu'ils soient, opèrent sur des infrastructures qui ne sont pas les leurs. Les modèles de fondation, la puissance de calcul, les composants électroniques et les couches logicielles restent, pour l'essentiel, sous contrôle américain¹⁵³.

Selon les estimations du Synergy Research Group, Amazon, Microsoft et Google concentraient environ 70 % du marché européen de l'infrastructure *cloud* en 2025, tandis que la part cumulée des fournisseurs européens plafonnait autour de 15 %¹⁵⁴. La dépendance est plus prononcée encore sur les logiciels d'entreprise : d'après une étude commandée par le Cigref,

149. V. Bansal, « Tech Workers Are Fighting Against Silicon Valley's AI Push », *Tech Policy Press*, 17 juin 2026 ; Q. Wong, « They Built AI: Now Silicon Valley Workers Protest Its Threat to Jobs and Humanity », *Los Angeles Times*, 22 juillet 2026.

150. N. Chapuis, « Aux États-Unis, l'opposition aux data centers grandit et devient un objet politique », *Le Monde*, 27 juillet 2026.

151. A. Pardes, « How AI May Drive Union-Resistant Tech Workers to the Bargaining Table », *The Guardian*, 21 juillet 2026.

152. I. Levingston *et al.*, « Investors Pour Billions into Europe's AI and Defence Start-Ups », *Financial Times*, 10 février 2026.

153. Il en va de même dans le champ industriel de l'IA, en dépit des multiples effets d'annonce publics comme privés. Les investissements massifs d'un acteur comme Mistral dans la construction de centres de données bénéficieront avant tout aux acteurs extra-européens qui les équiperont, voire en auront l'usage. Voir A. Piquard, « Microsoft signe un accord de "plusieurs milliards" de dollars pour utiliser les data centers de Mistral AI », *Le Monde*, 21 juillet 2026.

154. Données du Synergy Research Group, citées dans K. Nicol-Schwartz, « These Four Charts Show How Reliant Europe Is on U.S. Digital Infrastructure », *CNBC*, 13 février 2026.

quelque 80 % des dépenses annuelles européennes en logiciels et *cloud* professionnels (soit près de 300 milliards de dollars) profitent à des fournisseurs américains¹⁵⁵. Sur les enjeux ayant trait à la matérialité physique (terres rares, puces graphiques et mémoire, serveurs et composants de stockage, équipements réseau...), la dépendance à des acteurs extra-européens est tout aussi élevée.

Ce déséquilibre a trouvé, en juin 2026, une illustration retentissante dans un exercice prospectif qui a rapidement essaimé dans les cercles bruxellois¹⁵⁶. Rédigé par un collectif de chercheurs européens en IA et publié sous forme de scénario, « Europe 2031 » met en scène une Europe affaiblie sur le plan économique, instable sur le plan politique et vassalisée sur le plan technologique, faute d'avoir investi à temps dans la puissance de calcul et les modèles frontières¹⁵⁷. Dans le scénario, l'Europe ne contrôle plus qu'environ 5 % de la puissance de calcul mondiale dédiée à l'IA, contre 80 % détenue par les États-Unis, lui laissant un très faible pouvoir de négociation face aux fournisseurs américains. Le récit culmine lorsque les États-Unis décident, en 2031, de prendre le contrôle du néerlandais ASML. L'Europe se retrouve alors face à trois options également défavorables : accepter le statut de protectorat américain, basculer vers la Chine ou décliner dans l'isolement.

L'écho rencontré par « Europe 2031 » a été amplifié par sa concordance avec l'actualité, car sa parution a précédé de peu la décision de l'administration américaine de restreindre temporairement l'accès étranger aux modèles Fable 5 et Mythos 5 d'Anthropic¹⁵⁸. Combinée aux enseignements tirés du différend entre Anthropic et le Pentagone au printemps, la séquence ressemble, pour l'Europe, à un avertissement de portée stratégique. Ainsi, même une entreprise américaine peut voir ses modèles requalifiés en instruments de puissance nationale par leur gouvernement, sans que leurs clients étrangers disposent du moindre recours.

Or, c'est précisément dans le domaine de la défense que cette dépendance est la plus critique. Un « patriotisme européen » de la *DefTech* reposant sur des infrastructures étrangères signifie que la souveraineté technologique est tributaire de fournisseurs eux-mêmes à la merci de leur propre gouvernement. Que Mistral AI entraîne ses modèles sur des puces américaines fabriquées à Taïwan avec des équipements néerlandais placés sous contrôle d'exportation américain, ou que les startups de défense européennes recrutent leurs talents grâce à des fonds transatlantiques peut paraître anecdotique. Pourtant, pris ensemble, ils démontrent le plafond structurel à l'ambition d'autonomie stratégique du continent. La question,

155. Asterès, *Technological Dependence on American Software and Cloud Services: An Assessment of the Economic Consequences in Europe*, mai 2025, disponible sur : www.cigref.fr.

156. A. Down, « A Viral Doomsday Scenario Aims to Shake Europe out of Its AI Complacency », *The Guardian*, 20 juin 2026.

157. D. Juijn *et al.*, « Europe 2031 », 11 juin 2026.

158. A. Sircar, « Anthropic Disabled Fable 5 and Mythos 5 After a U.S. Export-Control Order. Here's What Happened », *Forbes*, 16 juin 2026.

dès lors, n'est plus tant de savoir si l'Europe peut se doter de champions de la *DefTech*, mais si elle peut le faire sans que la souveraineté qu'elle prétend reconquérir dans le domaine militaire ne se dissolve dans les couches inférieures de son *stack* technologique.

À cette dépendance d'infrastructure s'ajoute une menace d'un autre ordre. Le virage militaire des géants américains de la *tech* et l'essor de leurs champions de la *DefTech* font en effet peser sur l'industrie européenne le risque d'un marché submergé par des systèmes américains à bas coût et produits en masse. Des entreprises comme Anduril revendiquent un modèle fondé sur la production de systèmes autonomes modulaires, logiciels avant d'être matériels, fabriqués en grande série à des prix défiant ceux des plateformes traditionnelles. Or ces acteurs ne se contentent plus d'exporter, ils s'implantent désormais au cœur même de la BITD européenne¹⁵⁹. En juin 2025, Anduril a ainsi scellé un partenariat stratégique avec l'allemand Rheinmetall pour co-développer et fabriquer en Europe des versions européennes de ses drones autonomes Barracuda et Fury, ainsi que des moteurs-fusées¹⁶⁰. Si les systèmes sont présentés comme construits *avec* les Européens et non seulement *pour* eux, afin de désamorcer la crainte de la dépendance, ce partenariat n'en permet pas moins au modèle industriel et à l'architecture logicielle d'Anduril de s'implanter en Europe, quand bien même l'assemblage y est localisé.

En dépit d'efforts marginaux d'émancipation¹⁶¹, ce partenariat n'est pas isolé. Il s'inscrit dans une vague d'implantations qui voient les principaux « *collaborative combat aircraft* » américains traverser l'Atlantique par le biais de partenariats industriels. General Atomics adapte par exemple son YFQ-42A pour une production en Allemagne, tandis qu'Airbus s'est associé à l'américain Kratos pour proposer une version européenne du drone XQ-58A Valkyrie¹⁶². Le risque, pour la *DefTech* européenne naissante, est donc d'être concurrencée sur son propre marché domestique par des acteurs disposant d'une avance d'échelle considérable. À lui seul, Anduril a ainsi généré en 2025 un chiffre d'affaires (2,1 milliards de dollars) supérieur à l'ensemble des levées de fonds de l'écosystème européen de la *DefTech* la même année¹⁶³.

159. Dans ce contexte, il faut craindre qu'une part des 150 milliards d'euros prévus par la Commission dans le cadre du programme SAFE — destiné à financer les capacités de défense des États membres — ne soit *in fine* captée par des acteurs extra-européens.

160. C. Casimiro, « Anduril, Rheinmetall Partner to Produce Drones, Propulsion for Europe », *The Defense Post*, 19 juin 2025.

161. On peut songer à la décision française de ne pas renouveler le contrat liant la DGSI à Palantir, afin de privilégier l'offre nationale de ChapsVision, ce qui pourrait, à terme, produire un effet d'entraînement auprès d'autres partenaires européens (Danemark, Pays-Bas). Voir « Pourquoi les gouvernements européens réévaluent-ils leurs accords avec Palantir ? », Euronews, 5 juin 2026.

162. C. Charpentreau, « Helsing Unveils CA-1 Europa, a European Autonomous Combat Jet », *Aerotime*, 25 septembre 2025.

163. F. Véron et T. Bodin, « Defense Tech: Who Owns Europe's Next Arsenal? », *Newfund Capital*, 19 mai 2026, disponible sur : <https://blog.newfundcap.com>.

Les récentes velléités de l'ex-ministre de la Défense ukrainien Mykhailo Fedorov – grand artisan de la part technologique de la guerre menée par son pays – de vouloir créer une nouvelle entreprise de *DefTech* de dimension européenne grâce à l'appui financier d'Alex Karp, disent bien toute la difficulté de parvenir à une émancipation pourtant nécessaire¹⁶⁴. Pour éviter l'écueil d'une dépendance accrue et valoriser son capital technologique certain, l'Europe se doit de stimuler et de construire une hybridation féconde entre la fiabilité de sa BITD traditionnelle et l'agilité de ses nouveaux entrants¹⁶⁵. Ce n'est qu'à ce compte qu'elle pourra espérer assurer sa sécurité sans renier ni ses prérogatives ni ses obligations.

164. « Ukraine's Fedorov Says Palantir CEO Will Be First Major Investor in New Defence Company », Reuters, 1^{er} septembre 2026.

165. A. Papaemmanuel et L. de Roucy-Rochegonde, « L'Europe face au tournant de la *DefTech* », *op. cit.*

Conclusion

L'évolution du cycle d'innovation depuis le domaine civil vers le domaine militaire semble acter une bascule durable et décisive. Au regard des trajectoires historiques exposées, ce virage militaire des acteurs de la *tech* ne constitue pas une surprise et pourrait même s'avérer consubstantiel à la Silicon Valley, dont les identités multiples cachent mal un héritage au long cours. En revanche, l'intensité de cette bascule et les enjeux stratégiques qu'elle implique tout à la fois pour la BITD traditionnelle, les États de moins en moins donneurs d'ordre, mais également pour les populations exposées aux dérives d'une dérégulation galopante, méritent d'être scrutés de près.

Dans un monde où le retour de la conflictualité à grande échelle redéfinit constamment les usages des technologies duales sur les champs de bataille, ces acteurs sont en effet susceptibles de tirer pleinement parti de l'ajustement de leur positionnement et d'exercer un pouvoir qu'Eisenhower n'aurait pu se représenter au temps de son discours d'adieu. Lui qui estimait alors que « la désastreuse ascension d'un pouvoir illégitime existe et persistera¹⁶⁶ » aurait sans doute été effrayé de voir son avertissement amplement dépassé par le réel auquel nous sommes aujourd'hui confrontés.

Cette ascension est à présent manifeste, stimulée par la financiarisation de la sphère militaire, qui ne demeure plus sous la seule garde de la puissance publique et laisse craindre une privatisation rampante du plus stratégique des secteurs. Si les phénomènes de circulation intenses et les démonstrations régulières de force des décideurs politiques peuvent donner le change, une telle privatisation n'en demeure pas moins profonde et préoccupante. Car la sédimentation d'un complexe techno-militaire, organisé conjointement autour des géants historiques de la *tech* et des nouveaux entrants de la *DefTech*, constitue un défi à la fois stratégique et démocratique. Nourrie par un gouvernement américain à la dérive, cette sédimentation a déjà eu de fortes incidences sur la conduite d'opérations extérieures comme intérieures aux États-Unis, abîmant encore un peu plus l'image du régime de la « démocratie occidentale » à travers le monde.

À l'échelle européenne, elle appelle à un nécessaire pas de côté pour parvenir à la fois à s'extraire des dépendances structurelles qu'elle engendre et à préserver le cadre des valeurs fondamentales de l'UE et l'exercice des libertés publiques. S'engouffrer dans la brèche creusée par le modèle américain pourrait ainsi s'avérer contre-productif sur les plans tant technologique, diplomatique-stratégique que démocratique. Car, en plus de produire des dépendances problématiques, la délégation mal maîtrisée de

166. Discours de fin de mandat de Dwight D. Eisenhower, *op. cit.*

compétences que ce modèle implique engendre, *in fine*, un affaiblissement de la puissance publique, aux antipodes du projet européen. S'y opposer nécessite cependant une prise de conscience collective à laquelle l'urgence des impératifs géopolitiques laisse jusqu'ici peu d'espace. Reste à savoir si les résistances internes à ce secteur, encore marginales, et les efforts d'autonomie modestes mais croissants déployés par l'Europe porteront leurs fruits à temps. Ceci afin d'éviter que l'engrenage d'une confrontation sino-américaine – ou toute autre déflagration d'ampleur équivalente – ne soit précipité par une bascule techno-militaire plus qu'amorcée, et potentiellement débridée.



27 rue de la Procession 75740 Paris cedex 15 – France

Ifri.org