JUIN
2025

In conver-sation with

Investir dans l'Aéronautique, la Défense, et la Cybersécurité à travers le Private Equity

HENRI MARCOUX

TIKEHAU CAPITAL

CE DOCUMENT, PRODUIT PAR TIKEHAU INVESTMENT MANAGEMENT, FILIALE DE GESTION D'ACTIFS DE TIKEHAU CAPITAL, NE CONSTITUE PAS UN CONSEIL EN INVESTISSEMENT NI UNE RECOMMANDATION D'INVESTISSEMENT.
TOUT INVESTISSEMENT COMPORTE DES RISQUES, Y COMPRIS, MAIS SANS S'Y LIMITER, LE RISQUE DE PERTE DE CAPITAL.

In conver-sation with

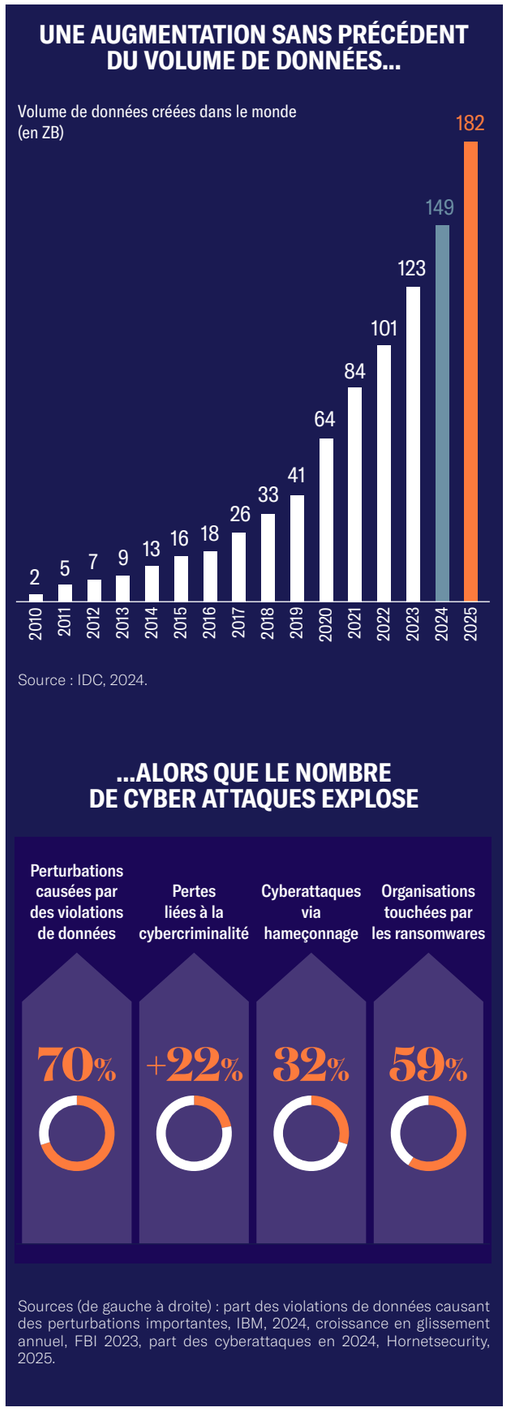
Henri Marcoux
Directeur Général Adjoint, Tikehau Capital

Investir dans l'Aéronautique, la Défense, et la Cybersécurité à travers le Private Equity

Chez Tikehau Capital, nous avons exprimé depuis la crise de la COVID-19 la conviction forte que la création de valeur économique dans le monde allait pivoter de la génération d'efficience à la génération de résilience. Après des décennies de baisse des taux d'intérêt et de mondialisation ayant permis aux acteurs économiques d'optimiser leur production, leurs chaînes d'approvisionnement et leur structure de capital, la démondialisation et les taux d'intérêt plus élevés poussent ces mêmes acteurs à renforcer leur robustesse en rapatriant la production proche du consommateur, en opérant avec des coussins de capitaux propres plus importants et en investissant massivement dans la création de résilience. La Cybersécurité, l'Aéronautique et la Défense sont des secteurs essentiels à la protection de notre modèle économique et à la souveraineté européenne : c'est pourquoi nous pensons qu'il est essentiel de soutenir leur croissance par le biais du Private Equity.

Quels sont les enjeux liés à la Cybersécurité ?

Les enjeux liés à l'explosion des usages numériques sont colossaux. Des secteurs critiques tels que les transports, l'énergie, la santé et la finance sont devenus de plus en plus dépendants des technologies numériques pour mener à bien leurs activités principales. Les entreprises doivent donc s'adapter à l'évolution des paradigmes des télécommunications et de l'informatique en numérisant leurs processus de production, leurs biens et services, leur distribution, leurs relations avec les clients et les partenaires et leurs chaînes d'approvisionnement. Au-delà d'une nécessité, il s'agit d'un facteur clé de la compétitivité. Les gouvernements sont également confrontés aux défis de la numérisation, notamment en termes de modernisation des services publics et d'amélioration de leur efficacité, des services de recherche d'emploi aux soins de santé, en passant par l'éducation et le paiement des impôts. Dans ce contexte, les défis de la Cybersécurité sont énormes. Si, d'un côté, elle est une nécessité pour la modernisation, un avantage concurrentiel et un élément clé du développement économique, elle apparaît aussi comme une extraordinaire source de vulnérabilité si les systèmes, les utilisateurs et les données ne sont pas correctement protégés. **Selon un rapport du Forum économique mondial, la cybercriminalité et la Cybersécurité figurent parmi les dix plus grands risques mondiaux, tant à court qu'à long terme[1].**



[1] https://reports.weforum.org/docs/WEF_Global_Risks_Report_2025.pdf

Dans ce contexte, les défis de la Cybersécurité sont énormes. Si, d'un côté, elle est une nécessité pour la modernisation, un avantage concurrentiel et un élément clé du développement économique, elle apparaît aussi comme une extraordinaire source de vulnérabilité si les systèmes, les utilisateurs et les données ne sont pas correctement protégés.

En effet, les économies se numérisent rapidement, la production de données explose et les cyberattaques deviennent plus fréquentes et plus sophistiquées. **Cette tendance devrait encore s'accentuer à l'avenir, car le nombre d'appareils connectés dans le monde devrait presque doubler, passant de 15,9 milliards en 2023 à plus de 32,1 milliards en 2030[2]. La Cybersécurité est devenue une mégatendance mondiale.**

En outre, des cadres réglementaires tels que la directive NIS2, la loi sur la cyber-résilience et le règlement DORA transforment le paysage, en particulier en Europe, et créent de nouveaux défis : selon le Forum économique mondial, 78% des dirigeants d'organisations privées estiment que les réglementations relatives à la cybernétique et à la protection de la vie privée réduisent efficacement les risques dans les écosystèmes de leur organisation[3]. Cependant, deux tiers des personnes interrogées ont cité la complexité et la prolifération des exigences réglementaires comme un défi.

[2] Source : Statista
[3] https://reports.weforum.org/docs/WEF_Global_Cybersecurity_Outlook_2025.pdf

Qu'en est-il de l'Aéronautique & la Défense ?

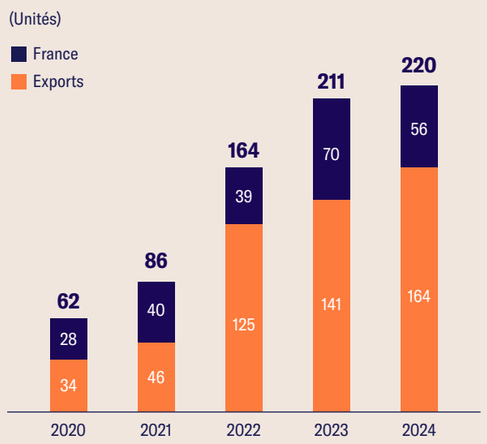
L'industrie de l'Aéronautique et de la Défense est par essence duale, avec une combinaison d'applications civiles et militaires. Cette dualité favorise l'innovation, permet des synergies entre les programmes de défense et les programmes commerciaux et préserve les compétences essentielles. À l'heure actuelle, les secteurs de la défense et de l'aviation commerciale sont tous deux confrontés au même défi : la nécessité d'augmenter rapidement les taux de production afin d'exécuter des carnets de commandes record :

Les carnets de commandes des industriels de la défense atteignent des niveaux record – par exemple, Dassault Aviation avait 220 Rafales en commande et n'a livré que 21 unités en 2024, ce qui nécessite une augmentation sans précédent des taux de production pour accélérer les livraisons[4]. Cette augmentation est due à l'aggravation des tensions géopolitiques et au besoin urgent de systèmes de défense modernisés et avancés. L'incapacité à augmenter rapidement la capacité de production pourrait mettre en péril les priorités de la sécurité nationale et retarder les déploiements de défense essentiels.

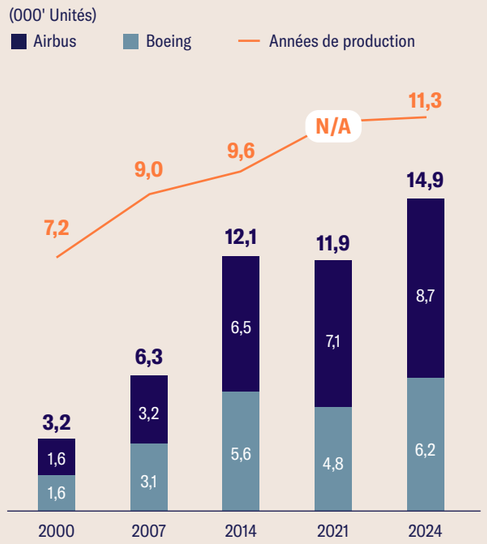
Les carnets de commandes commerciaux sont également bien remplis et sont restés très résistants pendant la crise : Airbus et Boeing ont 10 ans de livraisons dans leurs carnets de commandes. Pour Airbus, les carnets de commandes s'élevaient à 8 700 appareils en décembre 2024, tandis que 766 appareils ont été livrés en 2024[5]. La flotte mondiale devrait presque doubler d'ici 2043, soutenue par la demande croissante du trafic aérien et la nécessité pour les compagnies aériennes de renouveler leur flotte[6].

Les niveaux record atteints en termes de carnets de commandes offrent selon nous une visibilité à long terme sur les perspectives de croissance du secteur.

COMMANDES EN COURS DE DASSAULT AVIATION



CARNET DE COMMANDES D'AIRBUS & BOEING



Source : Information publique, Airbus et Boeing, 31 mars 2025.

[4] Source : Dassault Aviation, janvier 2025
[5] Source : Airbus et Boeing, décembre 2024
[6] Source : Airbus

À l'heure actuelle, les secteurs de la défense et de l'aviation commerciale sont tous deux confrontés au même défi : la nécessité d'augmenter rapidement les taux de production afin d'exécuter des carnets de commandes record

Quelles sont les opportunités d'investissement dans ces secteurs pour le Private Equity ?

La Cybersécurité, ainsi que l'Aéronautique & la Défense sont des domaines clés dans lesquels les entreprises du monde entier doivent investir massivement pour réduire leur vulnérabilité et renforcer leur résilience.

En ce qui concerne la Cybersécurité, McKinsey a estimé que la valeur du marché mondial de la Cybersécurité en 2024 aurait atteint jusqu'à 2 000 milliards de dollars, ce qui suggère une pénétration du marché d'environ 10%[7]. De même, la taille du marché mondial de la Cybersécurité était évaluée à 194 milliards de dollars en 2024 et devrait croître à un taux de croissance annuel moyen de 14,3% entre 2024 et 2032[8].

Il ne s'agit pas d'investissements tactiques, mais de choix stratégiques faits au niveau de la direction qui affectent tous les départements de l'organisation dans tous les secteurs d'activité, surtout si l'on met en perspective les 10 300 milliards de dollars que coûtera annuellement la cybercriminalité dans le monde en 2025, soit une multiplication par 10 par rapport aux niveaux de 2018[9]. Quels que soient la taille et le secteur, tout le monde est exposé au risque, et certaines industries/institutions font l'objet d'attaques répétées[10].

[7] « Data defense », McKinsey 2025.
[8] Fortune Business Insights, 2025.
[9] Statista Technology Market Insights, 2024.
[10] Parachute. Statistiques sur les cyberattaques en 2025. En date du 7 avril 2025.

ZOOM SUR
LES INDUSTRIES/INSTITUTIONS QUI FONT L'OBJET D'ATTAQUES RÉPETÉES[11] :

La santé
Le secteur a connu les violations de données les plus coûteuses depuis 13 ans. Au cours des quatre dernières années, les coûts ont même augmenté de 53,3%.

Les gouvernements
CyberArk prévoit que 60% des entités mondiales réglementées auront du mal à se conformer aux exigences en matière de protection des données et de divulgation des violations d'ici à 2026.

La finance
Le secteur financier est le deuxième plus touché par les violations de données sur le plan financier, avec un coût moyen par attaque de 8 millions de dollars.

L'énergie
Les cyberattaques coûtent au secteur de l'énergie 5,3 millions de dollars par incident en moyenne (2024).

[11] Source : Tikehau Capital, Baromètre des investissements européens dans la Cybersécurité, mars 2025.

Les entreprises les mieux organisées dans ce domaine, c'est-à-dire celles qui bénéficient d'un cyber-engagement de la part de la direction générale, d'un bon niveau de fiabilité des données et d'une organisation efficace, disposent d'une marge de progression beaucoup plus importante que les autres dans le domaine de la Cybersécurité.

Cependant, le secteur de la Cybersécurité est composé d'un grand nombre de start-ups et de moyennes entreprises non cotées financées par des fonds privés, principalement américains, bien que l'Europe émerge comme un leader de l'investissement non coté dans le secteur. Outre ces petites entreprises, un nombre limité de grands groupes cotés en bourse complètent le paysage de la Cybersécurité. **Cet écosystème en pleine croissance n'est pas encore mature : 7,1 millions de personnes travaillent actuellement dans la Cybersécurité dans le monde, mais 2,8 millions de postes ne sont pas pourvus, ce qui représente un taux de vacance de 28%.** Il y a une pénurie mondiale d'experts en Cybersécurité, en particulier dans quatre secteurs qui représentent 64% de la pénurie de main-d'œuvre en Cybersécurité[12] : les services financiers, les matériaux et l'industrie, les biens de consommation et la technologie.

Les besoins d'investissement dans ce domaine sont donc considérables, en particulier par le biais du Private Equity, étant donné que le secteur est principalement constitué d'entreprises non cotées en bourse. Les investissements mondiaux en capital-investissement et en capital-risque dans la Cybersécurité ont atteint 950 millions de dollars pour 21 transactions jusqu'à présent en 2025 et sont bien placés pour dépasser les niveaux de 2024[13].

> **Les investissements mondiaux en capital-investissement et en capital-risque dans la Cybersécurité ont atteint 950 millions de dollars pour 21 transactions jusqu'à présent en 2025 et sont bien placés pour dépasser les niveaux de 2024[13].**

Les investissements peuvent être réalisés sur l'ensemble de la chaîne de valeur de la Cybersécurité : dans des solutions de Cybersécurité pure, dans des technologies en amont qui accélèrent l'innovation en matière de Cybersécurité, et dans des technologies en aval, c'est-à-dire des applications commerciales qui mettent en avant leur niveau de sécurité comme un élément clé de différenciation.

En ce qui concerne les critères d'investissement, les entreprises qui ont des technologies éprouvées, des modèles de revenus avec une visibilité claire sur l'atteinte de la rentabilité et un avantage concurrentiel, et qui sont dirigées par des équipes capables d'assurer une croissance interne et externe, tendent à être les mieux positionnées pour se développer de manière durable.

[12] https://web-assets.bcg.com/61/d3/705fbd684d70b0e5f98cdcf7cf47/2024-cybersecurity-workforce-report.pdf.
[13] Source : « Private equity inflows to cybersecurity soar as Google's $32B deal adds tailwind » S&P Global.

Dans le domaine de l'Aéronautique & la Défense, certaines sociétés cotées en bourse bénéficient d'une visibilité sur les perspectives de croissance du secteur, comme Rheinmetall[14], qui vise à augmenter considérablement son carnet de commandes de 55 milliards d'euros à la fin de 2024 à 80 milliards d'euros d'ici à la fin de 2025. Cette entreprise allemande a également pour objectif de doubler son chiffre d'affaires pour atteindre 20 milliards d'euros en 2027, et de réaliser une marge opérationnelle de 18% en 2027[15]. Par ailleurs, **Safran** anticipe s une progression soutenue de ses activités dans les prochaines années, avec une augmentation des livraisons de moteurs Leap de 15 à 20% en 2025 par rapport à 2024, pour atteindre 2 000 unités en 2026 et environ 2 500 en 2028. Sur trois ans, les ventes de moteurs Leap devraient ainsi croître de 66%, accompagnées d'une hausse encore plus marquée des activités de maintenance et de services après-vente[16].

Pour continuer à augmenter les cadences de production, les grands fabricants doivent pouvoir s'appuyer sur une chaîne d'approvisionnement solide, elle-même capable d'augmenter la capacité de production et d'accélérer les livraisons.

Cette accélération sans précédent des cadences de production nécessite des capitaux massifs pour renforcer les bilans des maillons clés de la chaîne d'approvisionnement, dont les niveaux d'endettement ont augmenté sur la période 2020-2022[17] et leur permettre ainsi de financer la croissance. Outre les gouvernements, les capitaux privés sont appelés à jouer un rôle essentiel à cet égard.

C'est là que le Private Equity entre en jeu, car il est essentiel de pouvoir financer des actifs stratégiques dans l'industrie de l'Aéronautique & la Défense, en ciblant les acteurs de niche qui sont leaders sur leurs marchés, ainsi que les plateformes de consolidation afin d'accroître la résilience de la chaîne d'approvisionnement.

Les investissements peuvent être réalisés sur l'ensemble de la chaîne de valeur, dans les matériaux (tels que le titane), la mécanique (pièces et assemblages critiques), l'électronique (circuits imprimés, optronique, sous-systèmes complexes) et les services (services de production, opérations).

Enfin, un élément clé de différenciation pour investir dans l'Aéronautique & la Défense, mais aussi dans la Cybersécurité par le biais du capital-investissement, est de bénéficier d'un écosystème d'experts. En effet, il est essentiel de posséder une connaissance approfondie des défis et et des innovations liés à ces secteurs.

> **C'est là que le Private Equity entre en jeu, car il est essentiel de pouvoir financer des actifs stratégiques dans l'industrie de l'Aéronautique & la Défense, en ciblant les acteurs de niche qui sont leaders sur leurs marchés, ainsi que les plateformes de consolidation afin d'accroître la résilience de la chaîne d'approvisionnement.**

[14] À des fins d'illustration uniquement, ne constitue pas un conseil en investissement.
[15] Source : Rheinmetall : Rheinmetall, rapport annuel 2024.
[16] Source : Safran, décembre 2024.
[17] https://www.tikehaucapital.com/~/media/Files/T/Tikehau-Capital-V2/documents/news-and-views/tikehau-focus-defence-en.pdf.

> **L'Union Européenne met de plus en plus l'accent sur la souveraineté numérique, ce qui implique de développer ses propres solutions de Cybersécurité et de réduire la dépendance à l'égard des fournisseurs de technologie étrangers. Cette tendance accroît la demande de technologies de Cybersécurité développées localement, ce qui fait des entreprises européennes de Cybersécurité des cibles d'investissement attrayantes.**

Au-delà de l'opportunité d'investissement, en quoi ces secteurs jouent-ils un rôle essentiel dans le renforcement de la souveraineté européenne ?

En ce qui concerne la Cybersécurité, le paysage géopolitique complexe de l'Europe, avec des menaces allant des cyberattaques par des hacktivistes parrainés par les États aux préoccupations croissantes concernant la souveraineté des données, a stimulé l'investissement dans les entreprises de Cybersécurité locales. **L'Union Européenne met de plus en plus l'accent sur la souveraineté numérique, ce qui implique de développer ses propres solutions de Cybersécurité et de réduire la dépendance à l'égard des fournisseurs de technologie étrangers.** Cette tendance accroît la demande de technologies de Cybersécurité développées localement, ce qui fait des entreprises européennes de Cybersécurité des cibles d'investissement attrayantes.

Au cours de la dernière décennie, le marché européen de la Cybersécurité a continué à s'imposer comme une opportunité d'investissement clé, avec une multiplication par 1,6 du nombre de levées de fonds et une multiplication par 12,5 des montants investis. En 2024, 134 entreprises européennes de Cybersécurité ont été acquises, dont 71% par des acteurs européens, soit une augmentation significative de 19% par rapport à 2023[18].

[18] Source : Tikehau Capital, Baromètre des investissements européens dans la Cybersécurité, mars 2025.

L'Aéronautique & la Défense ne sont pas en reste. Depuis plus d'une décennie, les pays européens ont généralement dépensé moins que la ligne directrice de l'OTAN de 2% du PIB pour la défense[19]. Toutefois, cette tendance évolue rapidement. En 2024, la moyenne des dépenses de défense des pays européens était passée à 2,2% du PIB, et les pays européens de l'OTAN s'accordent pour atteindre 3% d'ici 2030[20], ce qui représente une augmentation significative par rapport aux années précédentes.

Cette augmentation reflète un consensus croissant entre les nations européennes en faveur d'engagements plus forts en matière de défense afin de répondre efficacement aux défis de sécurité émergents et aux tensions géopolitiques, en particulier à la lumière des récents conflits mondiaux et des instabilités régionales.

La Commission européenne a fait un pas dans cette direction en dévoilant un plan global pour réarmer l'Europe (ReArm Europe/Readiness 2030), avec l'objectif ambitieux de mobiliser 800 milliards d'euros d'investissements dans la défense au cours des prochaines années. Ce plan prévoit de stimuler les acquisitions communes, d'améliorer la recherche et le développement et de renforcer la base industrielle de défense européenne.

Parmi les pays européens, l'Allemagne fait figure d'acteur majeur. Elle est en passe de devenir le quatrième pays au monde en termes de dépenses de défense, après les États-Unis, la Chine et la Russie[21]. La croissance du budget de la défense de l'Allemagne souligne son rôle central dans la sécurité européenne et son engagement à atteindre des objectifs de dépenses plus élevés.

En outre, tous les pays européens cherchent activement à mobiliser des fonds supplémentaires pour renforcer leurs écosystèmes de défense. Il s'agit notamment d'augmenter les investissements dans les technologies de pointe, le renseignement et la modernisation des forces armées. Cet effort coordonné reflète une évolution stratégique vers une plus grande autonomie et une plus grande résilience du dispositif de défense de l'Europe.

En outre, tous les pays européens cherchent activement à mobiliser des fonds supplémentaires pour renforcer leurs écosystèmes de défense. Il s'agit notamment d'augmenter les investissements dans les technologies de pointe, le renseignement et la modernisation des forces armées. Cet effort coordonné reflète une évolution stratégique vers une plus grande autonomie et une plus grande résilience du dispositif de défense de l'Europe.

[19] https://www.mckinsey.com/industries/aerospace-and-defense/our-insights/a-different-lens-on-europes-defense-budgets.
[20] https://www.ft.com/content/c4942166-c61b-46ec-832f-1671aecf1b02.
[21] Source : Tikehau Capital, Tikehau Focus « Investing in defence across the entire value chain ».

Conclusion

Nous pensons qu'investir dans les secteurs de l'Aéronautique, de la Défense et de la Cybersécurité par le biais du Private Equity représente l'une des opportunités les plus importantes des prochaines décennies. Ces secteurs sont non seulement essentiels à la résilience économique et à la sécurité nationale, mais ils sont également à la pointe de l'innovation technologique et de la transformation industrielle. La numérisation rapide des économies, la complexité croissante des cybermenaces et le besoin urgent d'étendre et de moderniser les capacités de production de l'Aéronautique & la Défense soulignent la nécessité d'un investissement stratégique soutenu.

Le Private Equity pourrait jouer un rôle essentiel dans ce contexte en fournissant les capitaux flexibles et à long terme nécessaires pour faire évoluer les entreprises prometteuses, renforcer les chaînes d'approvisionnement et accélérer l'innovation, en particulier sur un marché où de nombreuses entreprises à forte croissance sont non cotées en bourse. En outre, ces investissements pourraient contribuer directement à renforcer la souveraineté européenne en réduisant la dépendance à l'égard des acteurs extérieurs et en encourageant le leadership technologique national[22].

[22] Ces opinions sont susceptibles d'être modifiées à tout moment et ne doivent pas être interprétées comme des conseils d'investissement, des recommandations de titres ou une indication de l'intention de négociation de la part de Tikehau Capital. Aucune prévision ne peut être garantie.

Ce document a été préparé par Tikehau Capital à des fins d'information uniquement. Il ne crée aucune obligation de la part de Tikehau Capital. Les informations contenues dans ce document ne constituent pas une sollicitation ou une offre à quiconque de souscrire, d'acheter ou de vendre des titres, des options, des parts de fonds ou tout autre instrument financier ou service, ni une recommandation d'effectuer un investissement ou une transaction. Il ne tient pas compte des objectifs d'investissement ou des besoins financiers du destinataire. Certaines informations économiques ou de marché contenues dans ce document proviennent de sources publiées par des tiers. Bien que ces sources soient considérées comme fiables, ni Tikehau Capital ni les membres de son équipe de gestion ne peuvent être tenus responsables de l'inexactitude de ces informations. Aucune action ne doit être entreprise ou omise sur la base de ce document. Tikehau Capital ne peut être tenu responsable de toute décision prise sur la base de ce document. Ce document n'a été approuvé par aucun organisme de réglementation. Pour plus d'informations, veuillez contacter Tikehau Capital : www.tikehaucapital.com

In conversation with

TIKEHAU CAPITAL

www.tikehaucapital.com