JUNE
2025

In conversation with

Investing in Aerospace, Defence and Cybersecurity through Private Equity

HENRI MARCOUX

TIKEHAU CAPITAL

In conver-sation with

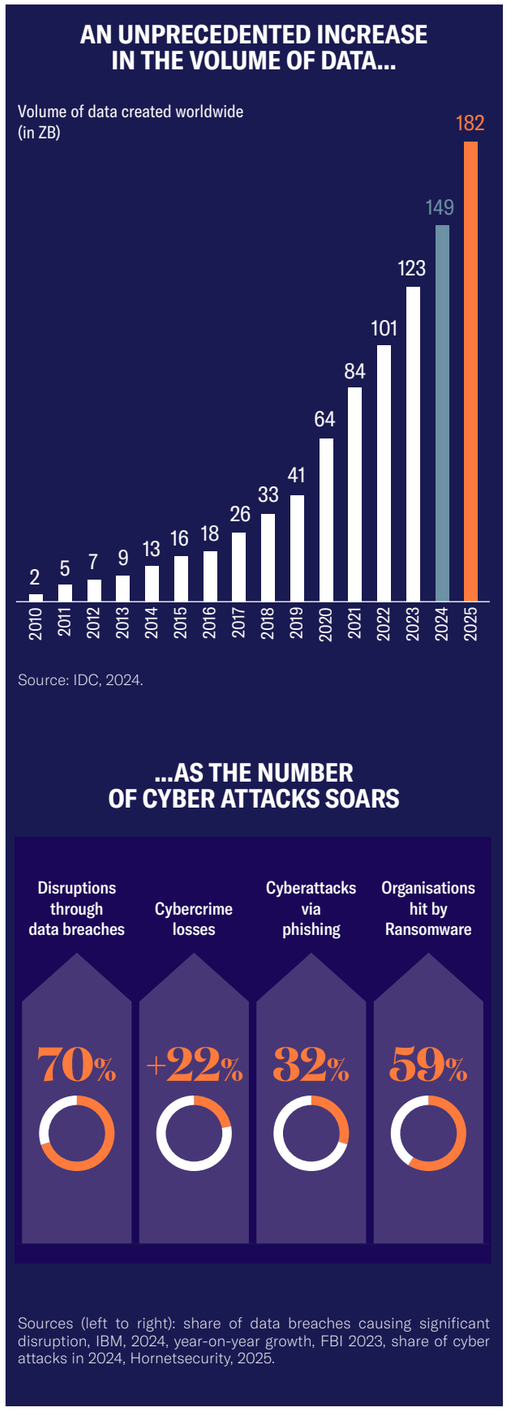
Henri Marcoux
Deputy CEO, Tikehau Capital

Investing in Aerospace, Defence and Cybersecurity through Private Equity

At Tikehau Capital, we have expressed a strong belief since the COVID-19 crisis that economic value creation around the world would pivot from the generation of efficiency to the generation of resilience. After decades of low interest rates and globalisation that allowed economic players to optimise their production, supply chains and capital structure, de-globalisation and higher interest rates are pushing these same players to strengthen their robustness by repatriating production close to the consumer, operating with larger equity cushions and investing massively in the creation of resilience. Cybersecurity, Aerospace and defence are key sectors for protecting our economic model and European sovereignty, which is why we believe it is essential to support their growth through Private Equity.

What are the challenges of Cybersecurity?

The challenges posed by the explosion in digital usage are colossal. Critical sectors such as transport, energy, health and finance are becoming increasingly dependent on digital technologies to carry out their core activities. Companies therefore need to adapt to changing telecommunications and IT paradigms by digitising their production processes, goods and services, distribution, relationships with customers and partners, and supply chains. More than just a necessity, it is a key factor in competitiveness. Governments are also faced with the digitisation challenges, particularly in terms of modernising public services and improving their efficiency, from job search services to healthcare, through to education and tax payments.
In this context, the challenges of Cybersecurity are enormous. While, on the one hand, it is a necessity for modernisation, a competitive advantage, and a key element of economic development, it also appears to be an extraordinary source of vulnerability if systems, users, and data are not properly protected. **According to a report by the World Economic Forum, cybercrime and cybersecurity are among the top ten global risks, both in the short and long term[1].**



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

> **In this context Cybersecurity challenges are enormous. If, on the one hand, it is a necessity for modernisation, a competitive advantage, and a key element of economic development, it also appears to be an extraordinary source of vulnerability if the systems, users and data are not properly protected.**

Indeed, economies are rapidly going digital, data production is exploding, and cyber-attacks are becoming more frequent and more sophisticated. **This trend is set to become even more pronounced in the future, as the number of connected devices in the world is expected to almost double, from 15.9 billion in 2023 to more than 32.1 billion in 2030[2]. Cybersecurity has become a global megatrend.**

In addition, regulatory frameworks such as the NIS2 directive, the law on Cyber resilience and the DORA regulation are transforming the landscape, particularly in Europe, and creating new challenges. According to the World Economic Forum, 78% of executives in private organisations believe that regulations on Cybersecurity and the protection of privacy effectively reduce risks in their organisation's ecosystems[3]. However, two thirds of respondents cited the complexity and proliferation of regulatory requirements as a challenge.

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

What about Aerospace & Defence?

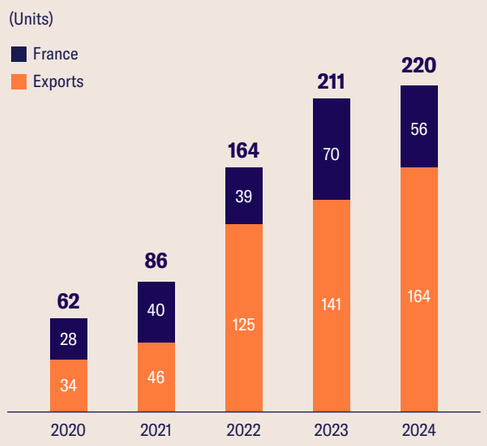
The aerospace and defence industry is inherently dual-use, with a combination of civil and military applications. This duality fosters innovation, enables synergies between defence and commercial programmes and preserves essential skills. Today, both the defence and commercial aviation sectors are facing the same challenge: the need to rapidly increase production rates in order to fulfil record order books:

Defence manufacturers' order books are at record levels - for example, Dassault Aviation had 220 Rafales on order and delivered only to 21 units by 2024, which will require an unprecedented increase in production rates[4] to speed up deliveries. This increase is due to heightened geopolitical tensions and the urgent need for modernised, advanced defence systems. Failure to rapidly increase production capacity could jeopardise the priorities of the European defence industry. national security and delay essential defence deployments.

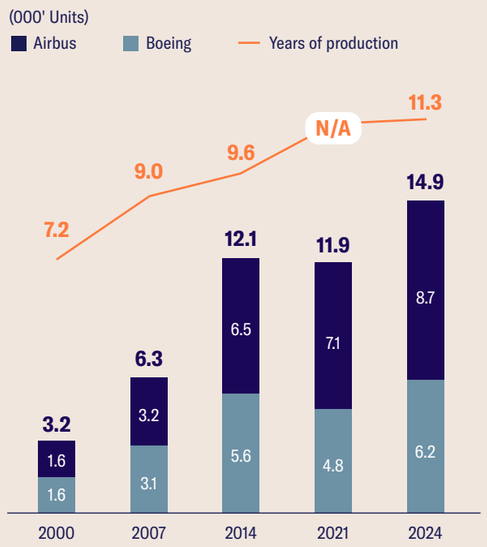
Commercial order books are also well filled and have remained very resilient during the crisis: Airbus and Boeing have 10 years of deliveries in their order books. For Airbus, order books stood at to 8,700 aircraft in December 2024, while 766 aircraft were delivered in 2024[5].

The world fleet is set to almost double by 2043, driven by growing air traffic demand and the need for airlines to to renew their fleet[6].

ORDER BOOKS FOR DASSAULT AVIATION



AIRBUS & BOEING ORDER BOOKS



Source: Public information, Airbus and Boeing, 31 March 2025.

[4] Source: Dassault Aviation, January 2025
[5] Source: Airbus and Boeing, December 2024
[6] Source: Airbus

Right now, defence sectors and commercial aviation are both faced with the same challenge: the need to rapidly increase production rates in order to deliver record orders.

What are the investment opportunities for Private Equity in these sectors?

Cybersecurity and Aeronautics & Defence are key areas in which companies around the world need to invest massively to reduce their vulnerability and strengthen their resilience.

With regard to Cybersecurity, McKinsey has estimated that the value of the global Cybersecurity market in 2024 will have reached up to 2,000 billion dollars, suggesting a market penetration of around 10%[7]. Similarly, the size of the global cybersecurity market was estimated at 194 billion in 2024 and is expected to grow at an average annual rate of 14.3% between 2024 and 2032[8].

These are not tactical investments, but strategic choices made at the top management level, that affect all departments of the organisation in all sectors business, especially if we put into perspective the $10.3 trillion annual cost of cybercrime in the world in 2025, a 10-fold increase on 2018 levels[9]. Regardless of size or sector, everyone is at risk, and certain industries/institutions are subject to repeated attacks[10].

[7] "Data defence", McKinsey 2025.
[8] Fortune Business Insights, 2025.
[9] Statista Technology Market Insights, 2024.
[10] Parachute. Statistics on cyber attacks in 2025. As of 7 April 2025.

ZOOM ON
INDUSTRIES/INSTITUTIONS WHICH ARE SUBJECT TO REPEATED ATTACKS[11]:

Healthcare
The sector has seen the most costly data breaches for 13 years. Over the last four years, costs have actually risen by 53.3%.

Governments
CyberArk predicts that 60% of global regulated entities will have to comply with data protection and breach disclosure requirements by 2026.

Finance
The financial sector is the second most affected by data breaches in financial terms, with an average cost per attack of $8 million.

Energy
Cyber attacks cost the energy sector an average of $5.3 million per incident (2024).

[11] Source: Tikehau Capital, European Cybersecurity Investment Barometer, March 2025.

The best organised companies in in this area, i.e. those that benefit from a cyber-commitment on the part of general management, a good level of reliability and efficient organisation, have much greater scope for progress than others in the field of Cybersecurity.

However, the Cybersecurity sector is made up of a large number of start-ups and medium-sized unlisted companies financed by private funds, mainly American, although Europe is emerging as a leader of unlisted investment in the sector. In addition to these small companies, a limited number of large listed groups complete the Cybersecurity landscape. **This ecosystem is not yet mature: 7.1 million people currently work in cybersecurity worldwide, but 2.8 million positions remain unfilled, representing a vacancy rate of 28%.** There is a global shortage of Cybersecurity experts, particularly in four sectors that account for 64% of the Cybersecurity workforce[12]: financial services, materials and industry, consumer goods and technology.

Investment needs in this area are therefore considerable, in particular through Private Equity, given that the sector is mainly made up of unlisted companies. Global private equity and venture capital investments in Cybersecurity reached 950 million euros for 21 transactions so far in 2025 and are well placed to surpass 2024 levels[13].

> **Global private equity and venture capital investments in Cybersecurity have reached $950 million in 21 deals so far in 2025 and are well placed to surpass 2024 levels[13].**

Investments can be made across the entire Cybersecurity value chain: in solutions Cybersecurity, in upstream technologies that accelerate innovation in terms of Cybersecurity, and in downstream technologies, i.e. commercial applications who emphasise their level of security as a key differentiator.

In terms of investment criteria, companies that have proven technologies, revenue models with clear visibility of profitability and competitive advantage, and that are led by teams capable of delivering internal and organic growth, tend to be the best positioned for sustainable growth.

[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.

In the aerospace and defence sector, certain listed companies benefit from visibility on the sector's growth prospects, such as Rheinmetall[14], which aims to significantly increase its order book from €55 billion at the end of2024 to €80 billion by the end of 2025. The German company is also aiming to double its revenue to €20 billion in 2027, and to achieve an operating margin of 18% in 2027[15]. Furthermore, **Safran** anticipates strong growth in its activities over the coming years, with deliveries of Leap engines expected to increase by 15 to 20% in 2025 compared to 2024, reaching 2,000 units in 2026 and around 2,500 in 2028. Over three years, sales of Leap engines are therefore expected to grow by 66%, alongside an even sharper rise in maintenance and after-sales service activities[16].

To continue to increase production rates, the major manufacturers need to be able to rely on a solid supply base, itself capable of increasing production capacity and accelerate deliveries.

This unprecedented acceleration in production rates requires massive amounts of capital to strengthen the balance sheets of the key links in the supply chain, whose debt levels have increased over the period 2020-2022[17] and enable them to finance growth. In addition to governments, private capital is set to play a key role in this.

That's where Private Equity comes in, because it is essential to be able to finance strategic assets in the Aerospace & Defence industry, targeting niche players that are leaders in their markets, as well as consolidation platforms to increase supply chain resilience.

Investments can be made throughout the value chain, in materials (such as titanium), mechanics (critical parts and assemblies), electronics (printed circuits, optronics, complex sub-systems) and services (production services, operations).

Finally, a key differentiator to invest in Aerospace & Defence, but also in Cybersecurity through private equity, is to benefit from an ecosystem of experts. Indeed, it is essential to have in-depth knowledge of challenges and innovations related to these sectors.

> **That's where Private Equity comes in, because it is essential to be able to finance strategic assets in the Aerospace industry & Defence, targeting niche players who are leaders in their markets, as well as consolidation platforms to increase resilience of the supply chain.**

[14] For illustrative purposes only, does not constitute investment advice.
[15] Source: Rheinmetall: Rheinmetall, Annual Report 2024.
[16] Source: Safran, December 2024.
[17] https://www.tikehaucapital.com/~/media/Files/T/Tikehau-Capital-V2/documents/news-and-views/tikehau-focus-defence-en.pdf.

> **The European Union is placing increasing emphasis on digital sovereignty, which means developing its own Cybersecurity and security solutions to reduce dependency on foreign technology suppliers. This trend is driving demand for locally developed Cybersecurity technologies, making European Cybersecurity companies attractive investment targets.**

In addition to the investment opportunity, how do these sectors play an essential role in strengthening European sovereignty?

When it comes to Cybersecurity, Europe's complex geopolitical landscape, with threats ranging from cyber-attacks by state-sponsored hacktivists to growing concerns about data sovereignty, has boosted investment in local Cybersecurity companies. **The European Union is placing increasing emphasis on digital sovereignty, which means developing its own Cybersecurity and security solutions to reduce dependency on foreign technology suppliers.**

This trend is driving demand for locally developed cybersecurity technologies, making European cybersecurity companies attractive investment targets. Over the past decade, the European Cybersecurity market has continued to grow. to become a key investment opportunity, with a 1.6-fold increase in the number of funds raised and a 12.5-fold increase in the amounts invested. In 2024, 134 European Cybersecurity companies were acquired, of which 71% from European players, a significant increase of 19% compared to 2023[18].

[18] Source: Tikehau Capital, European Cybersecurity Investment Barometer, March 2025.

Aerospace & Defence are not to be outdone. For more than a decade, European countries have generally spent less than NATO's guideline of 2% of GDP on defence[19]. However, this trend is changing rapidly. By 2024, average Defence spending by European countries had risen to 2.2% of GDP, and the European NATO countries have agreed to reach 3% by 2030[20], which represents a significant increase compared to the previous years.

This increase reflects a growing consensus among European nations in favour of stronger defence commitments in order to respond effectively to emerging security challenges and geopolitical tensions, particularly in the light of recent global conflicts and regional instabilities.

The European Commission has taken a step in this direction by unveiling a comprehensive plan to rearm Europe (ReArm Europe/Readiness 2030), with the ambitious aim of mobilising €800 billion in defence investment over the next few years. This plan includes stimulating joint acquisitions, improving research and development, and strengthening the European defence industrial base.

Among European countries, Germany is a major player. It is well on the way to becoming the fourth largest country in the world in terms in defence spending, after the United States, China, and Russia[21]. The growth in Germany's defence budget underlines its central role in European security and its commitment to higher spending targets.

In addition, all European countries are actively seeking to mobilise additional funds to strengthen their defence ecosystems. This includes increased investment in cutting-edge technologies, intelligence, and the modernisation of the armed forces. This coordinated effort reflects a strategic shift towards greater autonomy and resilience in Europe's defence posture.

In addition, all European countries are actively seeking to raise additional funds to strengthen their defence ecosystems. In particular, the aim is to increase investment in cutting-edge technologies, intelligence, and the modernisation of armed forces. This coordinated effort reflects a strategic shift towards greater autonomy and resilience in Europe's defence posture.

[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

We believe that investing in the Aerospace, Defence and Cybersecurity sectors through Private Equity represents one of the most important opportunities of the coming decades. Not only are these sectors essential to economic resilience and national security, they are also at the forefront of technological innovation and industrial transformation. The rapid digitisation of economies, the growing complexity of cyber threats and the urgent need to expand and modernise Aerospace & Defence production capabilities underline the need for sustained strategic investment.

Private equity could play a key role in this context by providing the flexible, long-term capital needed to grow promising businesses, strengthen supply chains, and accelerate innovation, particularly in a market where many high-growth companies are unlisted. In addition, these investments could contribute directly to strengthening European sovereignty by reducing dependence on external players and encouraging national technological leadership[22].

[22] These opinions are subject to change at any time and should not be construed as investment advice, securities recommendations or an indication of trading intent on the part of Tikehau Capital. No forecast can be guaranteed.

In conversation with

TIKEHAU CAPITAL

www.tikehaucapital.com