Supply growing faster than demand

Jean Langlois-Berthelot and Christophe Gaie

Faced with the explosion in cyberattacks, the profusion of new solutions sometimes gives the impression of an artificial frenzy, or even the creation of a bubble. It is not a bubble in the traditional sense: the threat is tangible, the incidents are real, and the sector is already generating substantial revenue and jobs. The economically relevant point is more specific. Certain segments of the supply side – particularly the most visible ones, comprising young software firms, the promises of platforms, narratives of sovereignty and, now, AI-driven solutions – are growing faster than the market's capacity to absorb them. A serious analysis of the economic situation of cybersecurity in France compares four sets of indicators: turnover, employment, the demographics of market players, and the speed at which demand is converted into purchases and performance. It is at this level that the current balance between the pace of technological innovation and the financing capacity of economic actors is changing in nature.

The statistical scopes are not entirely consistent across different sources, which necessitates a structural analysis. In 2023, the Directorate-General for Enterprises (DGE) estimated the French cybersecurity sector's turnover at 10.45 billion euros and its workforce at 50,000[1]. The Alliance for Digital Trust's (ACN) 2025 Observatory, using a broader definition of 'digital trust', estimates revenues of 21.3 billion euros and 107,000 jobs in 2024, with an average annual growth rate of 7 per cent since 2018, compared with 0.8 per cent for French GDP over the same period; cybersecurity accounts for 53 per cent of total turnover[2] . Even taking into account changes in the scope of measurement, the scale is clear: the economic foundation exists. France is

[1] Government. (2024). Cybersecurity. Directorate-General for Enterprise. https://www.entreprises.gouv.fr/secteurs-dactivite/le-secteur-du-numerique-en-france/la-cybersecurite

[2] ACN. (2025). Digital Trust Sector Observatory. https://www.confiance-numerique.fr/wp-content/uploads/2025/06/observatoire-acn-2025-de-la-confiance-numerique.pdf

therefore not facing a speculative fiction, but a real, already structured market.

It is precisely for this reason that the current discrepancy deserves to be taken seriously. The national cybersecurity strategy announced in 2021 allocated 1 billion euros, of which 720 million was public funding, with the aim of growing the sector from 7.3 to 25 billion euros and increasing employment from 37,000 to 75,000 by 2025[3] . Three years later, the DGE's estimate puts the cybersecurity market at 10.45 billion in 2023, whilst the ACN Observatory estimates the broader market at just 21.3 billion in 2024. Public ambition has therefore progressed faster than the economic scale actually achieved. The issue is not the existence of the sector, but the alignment between the dynamics of supply and the actual depth of the market.

A. A ROBUST INDUSTRY, BUT A START-UP SECTOR THAT IS STRUGGLING TO GAIN TRACTION

The first mistake in perspective is to portray French cybersecurity as a story of software and platforms. The sector's economic base remains, structurally, a service economy. The ACN Observatory estimates cybersecurity services at €5.036 billion, 29,271 jobs and 717 companies in 2024, of which 2.189 billion is for auditing, planning and consultancy, 1.614 billion for implementation, and 1.119 billion for securing managed services and operations. Cybersecurity products, meanwhile, account for 24,641 jobs[4] . These figures show that cybersecurity in France is primarily an industry of integration, auditing, operations and compliance. The start-up sector is not its economic core, but it is its most visible periphery.

Yet it is precisely this fringe that is beginning to show signs of local imbalance. The Wavestone–Bpifrance 2025 Radar lists 179 start- ups and 46 scale-ups in the cybersecurity sector in France, compared with 168 start-ups and 42 scale-ups a year earlier. At first glance, the growth appears robust. But the details are less flattering. The start-ups on the radar now employ just 1,685

[3] Ministry of the Economy, Finance and Recovery. (2021). Cybersecurity: the Government's efforts to strengthen protection for citizens, public authorities and businesses. https://www.economie.gouv.fr/cybersecurite-renforcement-gouvernement-protection-citoyens-administrations-entreprises

[4] ACN. (2025). Digital Trust Sector Observatory. https://www.confiance-numerique.fr/wp-content/uploads/2025/06/observatoire-acn-2025-de-la-confiance-numerique.pdf

people in 2025, compared with 1,687 in 2024. In other words, the number of players is increasing, but not employment within the youngest tier. The average size of a start-up on the radar thus falls from just over 10 employees to fewer than 9.5 in a year. Even more worrying, 70% of these start-ups have fewer than 10 employees, compared with 67% the previous year, whilst the proportion of those with more than 20 employees drops from 12% to 7%[5] . Even taking into account the selection biases inherent in this type of survey, the picture remains clear: the number of players is growing faster than their economic weight.

An analysis of funding confirms this interpretation. The total amount raised by the French cybersecurity ecosystem amounted to 289 million euros between June 2024 and May 2025[6] , compared with 229 million the previous year. Taken in isolation, this figure appears reassuring, particularly as French Tech as a whole raised €7.4 billion in 2025, down 5 per cent in value and 15 per cent in volume. However, the key factor is not the total, but its distribution. In cybersecurity, the number of funding rounds fell from 29 to 19 in one year. Smaller funding rounds, an indicator of the depth of seed funding, contracted significantly: nine rounds of less than 10 million, totalling 17 million euros in 2025, compared with twenty-one rounds totalling 56 million in 2024. Conversely, ten funding rounds exceeding 10 million account for the bulk of the funding, and France remains virtually absent from rounds exceeding 30 million. The market therefore does not appear to be expanding but rather becoming polarised[7] .

This polarisation would be less problematic if it were accompanied by clear industry consolidation. However, the *turnover* of players reveals the opposite. In 2025, 43 start-ups entered the radar and 33 left it. Among the exits, there were 11 business closures and 8 acquisitions[8] , compared with just one acquisition the previous year. The market is already undergoing a process of natural selection. Above all, the new entrants are concentrated in clearly defined functional areas such as application security, anti-fraud,

[5] Wavestone–Bpifrance. 2025 French Cybersecurity Start-up Radar: with 179 start-ups and 46 scale-ups, the French ecosystem continues to grow, albeit at a slower pace. BpiFrance. https://presse.bpifrance.fr/radar-des-startups-cybersecurite-francaises-2025-avec-179-startups-et-46-scale-ups-lecosysteme-francais-poursuit-sa-croissance-malgre-un-rythme-moins-soutenu/?lang=fra

[6] Ibid.

[7] Ibid.

[8] Ibid.

governance, artificial intelligence and vulnerability management. These new entrants are focusing on segments that are already heavily occupied, which is problematic because an ecosystem that attracts new players to the same layers creates redundancies faster than it opens up new spaces.

The case of AI is particularly illuminating. The Radar 2025 indicates that 53 per cent of start-ups and scale-ups now incorporate AI into their offering, 30 per cent use it to automate or accelerate cybersecurity measures, and 15 organisations are specifically positioning themselves around securing AI uses or models, compared with 11 a year earlier. This thematic expansion is logical but, in a market that is genuinely maturing, it should be accompanied by a strengthening of industrial evidence. However, such evidence remains concentrated. Only 15 per cent of start-ups hold at least one cybersecurity certification, compared with 49 per cent of scale-ups. Internationalisation acts as a further indicator, with 61 per cent of organisations exporting, and as many as 93 per cent among scale-ups. The main divide therefore does not separate innovation from conservatism; rather, it distinguishes between players capable of expanding their offering beyond the domestic market and those who still depend on it.

It is important to assess what this means in economic terms. The 46 scale-ups on the radar account for a total of 4,483 jobs, compared with 1,685 for the 179 start-ups. The bulk of this innovative sector therefore rests on a limited number of already established players. The current dynamic reflects less a uniform deepening of the market than a phase of selection. A few trajectories are gaining momentum, whilst the base is fragmenting.

B. THE REAL BOTTLENECK IS ABSORPTION

This assessment is not based on weak demand. On the contrary. ANSSI handled 4,386 security incidents in 2024, a 15 per cent increase year-on-year. Its 2025 overview identifies 196 incidents involving data exfiltration, compared with 130 in 2024[9]. CESIN estimates that 40% of large organisations suffered at least one significant attack in 2025, and that 81% of victims

[9] ANSSI. (2025). 2024 Cyber Threat Overview: Mobilisation and Vigilance Against Attackers. https://cyber.gouv.fr/actualites/panorama-de-la-cybermenace-2024-mobilisation-et-vigilance-face-aux-attaquants/

experienced an impact on their operations[10] . The need is real, constant and measurable.

However, this need does not automatically translate into a thriving market for the entire range of solutions on offer. Among large enterprises, regulatory pressure is immense: 85 per cent of companies report being subject to at least one piece of cybersecurity legislation, including 59 per cent to NIS2, 32 per cent to DORA and 30 per cent to the Cyber Resilience Regulation[11] . Yet this pressure does not automatically lead to efficient resource allocation. The EY–Hexatrust barometer shows that 49 per cent of organisations have not defined an action plan for these frameworks, 40 per cent do not monitor sovereign solutions at all, and whilst 75 per cent are aware of the sector's certification schemes, only 47 per cent use them as a purchasing criterion[12]. Practice is therefore adapting more slowly than the discourse on sovereignty is developing.

The most critical factor is operational capacity. The CESIN–I-Tracing study from April 2026 shows that 85 per cent of organisations use at least two tools to track vulnerabilities, and 15 per cent use five or more; 24 per cent still manage this partially via shared files, 22 per cent have neither a dashboard nor a dedicated tool, and only two in five organisations have a cross-functional prioritisation process. At the same time, critical vulnerabilities are exploited within 24 to 48 hours, but fewer than 8 per cent are patched within 24 hours[13] . Whilst the capabilities to detect cyberattacks exist, their remediation is less clear-cut. This seems to indicate that the cybersecurity ecosystem generates more visibility than it does actual risk reduction.

CESIN documents the same discrepancy from another angle. Phishing remains the leading attack vector at 55 per cent, ahead of vulnerability

[10] CESIN. (2026). 11th edition of the CESIN Annual Barometer. https://cesin.fr/document.php?d=69772cd352310

[11] EY and Hexatrust. (2025). 2025 Digital Sovereignty Barometer. https://www.ey.com/content/dam/ey-unified-site/ey-com/fr-fr/services/cybersecurity/documents/ey-barometre-de-la-souverainete-numrique-sep-2025.pdf

[12] EY–Hexatrust Barometer (2025). Cybersecurity and Sovereignty: Where Do French Companies Stand? https://www.ey.com/fr_fr/insights/cybersecurity/cybersecurite-et-souverainete-ou-en-sont-les-entreprises-francaises

[13] CESIN–I-Tracing. (2026). Vulnerability management: How to reduce your exposure to cyberattacks. https://cesin.fr/document.php?d=69d5029a53a29

exploitation at 41 per cent and attacks via third parties at 35 per cent[14] . One-third of organisations estimate that more than half of their incidents originate from third parties. However, 81% of companies believe they have complete visibility over their assets, but this confidence drops to 31% for cloud environments. Blind spots persist regarding privileged access, subcontractors and hybrid environments. These factors confirm a lack of effective integration of the solutions available on the market.

The situation for SMEs and mid-market companies exacerbates this gap. 82 per cent leave IT management to the business owner, 72 per cent have no dedicated staff, 68 per cent spend less than 2,000 euros a year on cybersecurity, and only 10 per cent plan to increase this budget[15] . This segment represents a considerable economic volume, but is not yet a viable market for complex solutions. It calls for simple, shared and managed models, rather than a proliferation of platforms.

Finally, the issue of sovereignty reveals a structural limitation. The European Union accounts for around a quarter of global cybersecurity purchases[16] , but only 5% of the global market[17]. EU demand exists, but it largely translates into revenue for non-European players. Without mechanisms to convert orders into domestic effort, the growth of the domestic supply does not guarantee industrial consolidation.

The Court of Auditors also emphasises that the national cybersecurity strategy has yet to be translated into detailed operational planning. Public intervention has played a legitimate catalytic role. However, an ecosystem

[14] CESIN. (2026). 11th edition of the CESIN annual barometer. https://cesin.fr/document.php?d=69772cd352310

[15] Cybermalveillance.gouv.fr. (2024). Cybermalveillance.gouv.fr, the EBIOS Club, the CPME, the MEDEF and the U2P launch ImpactCyber to encourage micro-enterprises and SMEs to improve their security. https://www.cybermalveillance.gouv.fr/tous-nos-contenus/actualites/cp-lancement-impactcyber

[16] GINEIKYTE-KANCLERE, V., EGGERT, M., SKIOTYTE, G., & Visionary Analytics. (2025). European software and cyber dependencies (By the European Parliament's Committee on Industry, Research and Energy (ITRE) & the European Parliament). https://www.europarl.europa.eu/RegData/etudes/STUD/2025/778576/ECTI_STU(2025)778576_EN.pdf

[17] European Commission. (2026). Proposal for a Regulation of the European Parliament and of the Council on a framework of measures for strengthening the Union's semiconductor ecosystem, repealing Regulation (EU) 2023/1781 (Chips Act 2.0) (COM(2026) 504). Directorate-General for Communications Networks, Content and Technology.

that has grown under public impetus faster than its commercial autonomy can be established remains vulnerable to adjustment.

Thus, the French cybersecurity sector does not exhibit the characteristics of a bubble in the traditional sense. It is underpinned by genuine demand, documented incidents and a solid economic foundation. However, the data point to a growing mismatch between the density of supply, the market's ability to distinguish between different offerings, and the actual generation of measurable defensive benefits. If the ecosystem consolidates its players, expands its teams, improves its operational indicators and converts more of its domestic demand, the current phase will appear to be a normal selection process. Otherwise, the proliferation of offerings will resemble less a deepening of the market than a saturation phase preceding consolidation.