2026

confiance-numerique.fr

Observatory of Digital Trust Sector

ACN

Alliance pour la confiance numérique

Inspire Unify Empower Act

ACN

Alliance pour la confiance numérique

Observatory of Digital Trust Sector

2026

Réalisation - Mise en page
Agence Verveine

finished printing in May 2026

SUMMARY

A WORD FROM ACN 4

A WORD FROM THE MINISTER 6

KEY INSIGHTS 8
- Key figures 2025 10
- Fundamentals 2025 12
- The main segments of digital trust in 2025 12
- Breakdown by company size 2025 13
- Growth in France: a comparison, 2017–2025 13
- Top players 2025 14
- Focus: digital Security Segment 16
- Focus: products and Solutions Segment 17
- Focus: cybersecurity Services Segment 18
- Focus: trusted AI Segment 19

1 • DIGITAL TRUST 21
- 1.1 Cybersecurity, Digital Security and Trustworthy AI: a complementary technological triptych 22
- 1.2 The ACN's purpose, missions and values 24
- 1.3 The Scope of Digital Trust - segmentation 25
- 1.4 Methodology 26

2 • AN IMPORTANT AND DYNAMIC INDUSTRY 28
- 2.1 The French sector with the strongest growth over the period 2016–2024 30
- 2.2 Digital Trust is the industrial sector whose activity creates the most wealth in France 31
- 2.3 Digital Trust is a fully-fledged french industrial secteur 32
- 2.4 French players are at the top level in terms of skills and R&D 33
- 2.5 The growth in Digital Trust is part of a global dynamic 33
- 2.6 Growing competition from foreign players 34
- 2.7 A sector with great potential if the right strategic choices are made 35

3 • KEY FIGURES FOR THE SECTOR 36
- 3.1 Size and growth 38
- 3.2 Number of companies 39
- 3.3 Jobs 40
- 3.4 Added value 41
- 3.5 Mergers and acquisitions 42
- 3.6 A slowdown in investment in 2024, which is set to continue into 2025 46
- Point of view: european Cybersecurity Investment Barometer 48
- 3.7 Strengthening SMEs and trends in the development of the start-up ecosystem 49
- Focus: public funding for innovative projects in the sector 52
- Point of view: Abbas Djobo's point of view 54

4 • TRUSTED AI: CHALLENGES AND PROSPECTS FOR THE FUTURE 56
- 4.1 The artificial intelligence value chain 58
- 4.2 AI for general or specific use: different data requirements 60
- 4.3 Specific AI generates more value than general-purpose AI in France 62
- 4.4 The rise of agent-based AI in cybersecurity 63
- Point of view: alignment: the key to trust in AI systems Vanina Paoli-Gagin – Senator for Aube 64

5 • CURRENT STATUS OF ONLINE THREATS 66
- 5.1 ANSSI Cyber Threat Overview 2025 68
- 5.2 Insights from industry experts 70
- Focus: DOCAPOSTE-CYBLEX Cybersecurity Barometer 2025 76

6 • MARKET TRENDS 78
- 6.1 General trends 80
- Focus: structuring the ecosystem to scale up – the role of the Cyber Campus 84
- Focus: overview of the Regional Cyber Campus Network 86
- 6.2 Regulatory trends 96
- Focus: the Digital Resilience Index: a tool for measuring digital dependencies 105
- Focus: actions in the context of the AI Summit – February 2025 106
- 6.3 Technology trends 109
- Focus: research: program agencies and cybersecurity 112

ABOUT ACN 122

SUMMARY
ACN Observatory of Digital Trust Sector 2026

A WORD FROM ACN
ALLIANCE FOR DIGITAL TRUST

Grégory Wintrebert
ACN Chairman

The release of the 12th edition of the ACN Observatory comes amid a particularly tense global and economic climate, where geopolitical crises, trade disruptions, and cyber threats are reshaping the contours of our sovereignty. These upheavals, amplified by inflationary pressures and structural vulnerabilities, are testing our digital value chains and tend to slow the growth rate of the digital trust sector, which nevertheless remains highly dynamic with 5.4% growth projected for 2025.

Nevertheless, this demanding environment compels us to rethink our models and accelerate our transition toward greater autonomy. The ACN Observatory, with its in-depth analyses and forward-looking perspectives, offers valuable insights to guide our collective decisions during this critical period.

Reaffirming digital trust in the face of current challenges

At the heart of this dynamic lies the French digital trust sector, which is essential for building resilient societies and high-performing economies while strengthening our digital sovereignty.

Our sector, which spans digital identity, cybersecurity, trusted AI, blockchain, and trusted digital infrastructures, is on the front lines in addressing these challenges.

By 2025, it represents nearly €35 billion in global revenue, including €22.4 billion in France, and employ more than 170,000 people worldwide, including 62,000 in France. In the coming years, the effective rollout of the European digital identity portfolio for citizens and businesses will mark a decisive step forward, while progress driven by French and European regulations (Resilience, NIS2, Cyber Resilience Act, etc.) will help consolidate our cybersecurity and strengthen our sector. Furthermore, the emergence of a legal framework for trustworthy AI will open new avenues for ethical, controlled, and inclusive innovation, based on trusted digital infrastructures.

“ACN is positioning itself at the heart of the national digital ecosystem by strengthening ties with public institutions and local authorities”

Our three strategic priorities: an ambitious roadmap

To address these challenges, the ACN is guided by three clear strategic priorities. First, we aim to structure the sector by optimizing initiatives and fostering collaboration. This means producing robust analyses, consolidating our data, clarifying the challenges of key markets, supporting companies in their compliance efforts, and promoting French and European expertise. This mission is embodied in our work, our successive Observatories, and our constant effort to provide the sector with a clear, coherent, and ambitious framework.

Second, we believe it is essential to unite stakeholders behind a unified voice, while preserving their unique characteristics.
Digital trust is never built in isolation. It relies on ongoing dialogue between providers, users, institutions, researchers, and public authorities. Our role is to build these bridges, promote the exchange of best practices, lead open and rigorous working groups, and speak with a collective voice capable of influencing national and European roadmaps. As evidenced by our recent initiatives, this dynamic of cooperation grows stronger year after year.

Finally, the ACN positions itself at the center of the national digital ecosystem, strengthening the already close ties with public institutions and local communities. In a context of regulatory consolidation, rising demands for digital trust, and global technological competition, we serve as an anchor. We are an active, influential, and proactive player. Our ability to engage with decision-makers, anticipate change, and guide both public and private strategies is at the heart of our mission.

These pillars guide our daily actions and amplify our collective impact. We have also devoted significant effort to formalizing our purpose, our missions, and our core values. These are crystallized around four action verbs: inspiring through innovative visions, bringing together the dynamic forces of the sector, strengthening our collective capabilities, and taking decisive action to achieve tangible results. This clear charter now guides all of ACN’s initiatives.

A profound transformation to serve the industry and the country

To best support the ongoing changes, ACN is expanding its scope. We are embarking on a profound evolution of our services to offer our members and the entire industry increased added value: enhanced analytical tools, personalized support, strategic knowledge generation, dedicated discussion forums, joint initiatives, and more.

Above all, as a professional association representing the sector, we are working to reinvent the relationship between businesses and public authorities, placing trust at the center of the relationship and proposing innovative partnership models in the service of digital sovereignty and national resilience. This ambition positions us as a pivotal player in building a controlled technological future and we will be proactive in vigorously advocating for the priorities of companies in our sector with the candidates in the upcoming presidential election.

We are entering a new era. Digital trust is being reinvented, expanding, and becoming more complex. The ACN is transforming itself in turn to support the sector through this transition. Together, we will strengthen our capacity for action, assert our role within the ecosystem, and lay the foundations for a sector that is ever stronger, more united, and more strategic for our country and Europe.

“Digital trust is being reinvented, expanding and becoming more complex”

A WORD FROM THE MINISTER

Anne Le Hénanff
Minister for Artificial Intelligence and the Digital Affairs

In a turbulent geopolitical context, digital technology stands out even more clearly as one of the essential prerequisites for our sovereignty, the key to taking control of our destiny.

I have made digital sovereignty the guiding principle of my work. This cannot be merely a slogan or a posturing. It is a compass that guides our choices and determines our ability to decide for ourselves. To be sovereign is, first and foremost, to face our technological dependencies head-on. This clarity is essential: we can only transform what we understand.

Based on this mapping, we must develop alternative solutions, with a sovereign, French, and European offering. This requires creating the conditions for these solutions to exist, particularly at the European level. It also involves embracing a form of European preference to strengthen our collective autonomy. At the national level, this is achieved through public and private procurement.

Digital sovereignty is not limited to an industrial or technological issue. It is inseparable from the defense of our values. Protecting citizens, particularly the most vulnerable, ensuring fair competition, and enforcing our rules against major platforms are fundamental requirements. I refuse to pit innovation against regulation: we must strike a balance, one that is demanding and responsible. Ultimately, digital sovereignty is a prerequisite for our strength, our independence, and the vitality of our democracy. It cannot be decreed; it is built over time.

Digital sovereignty and innovation go hand in hand. This is particularly true in the field of artificial intelligence. The development of artificial intelligence is a major challenge for our society: AI represents a major opportunity for our businesses, our research labs, and our communities, all of which can boost productivity by automating certain tasks, freeing up time for employees to focus on high-value-added work. Those that fail to adopt it, on the other hand, risk being quickly overtaken by their competitors. That is why we are taking action to ensure that all our businesses adopt AI, through a national plan: “Dare to Embrace AI.”

“AI presents a major opportunity for our businesses, our research centres and our local authorities”

But this development can also be cause for concern: the risks associated with AI are numerous. The development of AI can have harmful consequences for work, the environment, and mental health. That is why we are taking action to ensure that, in France and across Europe, we have AI systems that reflect who we are, align with our values, and do not endanger our people or our planet.

While technological progress certainly brings opportunities, it must go hand in hand with the enactment of an ambitious digital security policy to counter its risks and potential abuses.

Cybersecurity is a challenge we must collectively address. As the 2025 National Strategic Review rightly pointed out, “cyberspace has become a space for competition, contestation, and sometimes even unrestrained confrontation, mirroring geopolitical tensions and international rivalries.” This observation reminds us that cybersecurity has become a sine qua non for our freedom, our sovereignty, and our strategic autonomy.

In this context, the State has developed an ambitious roadmap for the Nation through the 2026–2030 National Cybersecurity Strategy, structured around five pillars to strengthen the Nation’s cyber resilience and align France’s actions with European and international frameworks to ensure the stability of cyberspace.
The next step in this regard will be the adoption of the Resilience Bill by the National Assembly, which will, for the first time, set ambitious cybersecurity requirements for 15,000 critical and important entities in accordance with the European NIS 2 Directive.
But the government’s word cannot be credible if it does not set strong ambitions for its own cybersecurity. It is in this spirit that the Prime Minister has, for the first time, made public the 2026–2027 interministerial roadmap on priority efforts regarding the state’s digital security.

Digital sovereignty also means ensuring that our fellow citizens operate in a digital space that respects our laws and regulatory framework. This is essential for the most vulnerable, particularly minors, but also for the protection of our democratic systems.

In light of the now clearly established risks that social media poses to the mental and physical health of minors, as well as to their safety, I am advocating, at both the national and European levels, for the establishment of a digital age of majority set at 15, prohibiting access to social media for those under this age.

At the same time, I have tasked the Council on Artificial Intelligence and Digital Technology with organizing and structuring scientific research on emerging risks related, on the one hand, to conversational assistants based on generative artificial intelligence and, on the other hand, to video games.

In anticipation of the 2027 elections, France has adopted a National Strategy to Combat Information Manipulation (2026–2030), one of whose objectives is to strengthen the regulation of online platforms and generative artificial intelligence services at the European level–an initiative I will champion at the European level in the coming months at the urging of the President of the Republic.
You can count on my full commitment to making digital technology one of the drivers of our country’s excellence.

“Cybersecurity has become an essential prerequisite for our freedom, our sovereignty and our strategic autonomy”

KEY FIGURES

- Key figures 2025
- Fundamentals 2025
- The main segments of digital trust in 2025
- Breakdown by company size 2025
- Growth in France: a comparison, 2017–2025
- Top players 2025
- Focus: digital Security Segment
- Focus: products and Solutions Segment
- Focus: cybersecurity Services Segment
- Focus: trusted AI Segment

The ACN has set up a **Digital Trust Observatory** to collect and share data on the key characteristics and trends within this sector; it was within this framework that this study was carried out in 2026, covering the fields of cybersecurity, digital security and AI. The key findings of the 2026 edition focus on the sector's revenue growth, the strengthening of its international presence, and the identification of the markets that remain the most promising.

Key figures in 2025

€22.4 B
Digital trust

+4,2%
Growth (exluding AI)

+5,4%
Growth (with AI)

+2,4%
Digital security

+5%
Cybersecurity

+23,4%
Trusted AI Fundraising
M&A

Fundraising M&A

#1 Digital Trust remains a growing sector, but the slowdown that began in 2023 is confirmed in 2025

After peaking in 2022, revenue growth is gradually slowing, dropping from 6.8% in 2023 to 6.4% in 2024, and then to 4.2% in 2025. However, when including artificial intelligence–the only segment posting double-digit growth–growth reaches 5.4% in 2025.

This deceleration is part of a broader market slowdown, marked by geopolitical tensions, increased strain on public finances, and growing pressure on organizational budgets. It is also linked to operational dynamics, including longer decision-making cycles, tensions in the consulting market, and intensified competition, particularly manifesting as price wars in certain segments.
It can also be explained by the contrasting performance of the segments:

- **digital security,** a more mature segment, continues to show moderate growth (+2.4% in 2024 and +2.4% in 2025)
- **cybersecurity** continues to play a leading role but with less consistent momentum, as cybersecurity products remain on a positive trajectory (+6.4% in 2025) while cybersecurity services slow significantly (+3.4% in 2025 after +10.6% in 2024).
- **Trusted AI** appears to be the most dynamic segment, with growth of 9.3% in 2024 and 23.4% in 2025.

In this context, market development continues to be driven by structural challenges surrounding artificial intelligence, resilience, and sovereignty. At the same time, the ecosystem continues to consolidate, although fundraising is declining (€456 millions for 41 deals in 2023, compared to €352 millions for 27 deals in 2024), reflecting a more selective investment environment.

These trends point to growth that remains strong but is now more selective, driven primarily by the most differentiated segments.

The industry's main markets :

18%
Public Sector

&

17%
Banking
Finance Insurance

#2 High-growth markets: growth drivers are concentrated in segments where security is least negotiable

Against a backdrop of a global slowdown, the most promising markets remain those where security, sovereignty and resilience are the least negotiable.
The main drivers of growth are therefore **defence, space, security, major government departments and affiliated bodies**, as well as banking and insurance. These markets continue to underpin demand, as they are directly subject to stringent requirements regarding business continuity, compliance, data protection and the management of critical infrastructure.
This polarisation of demand primarily benefits those players best positioned to meet critical or differentiating needs. It explains why, despite the overall slowdown in the sector, certain SMEs and mid-market companies continue to record double-digit growth, particularly when they offer high-value-added solutions underpinned by sovereign, regulatory or sector-specific requirements that are difficult to postpone.
Growth is concentrated in the most critical segments, where security, compliance, and sovereignty are becoming dominant purchasing criteria, limiting budget trade-offs and accentuating polarization at the expense of more standardized and easily substitutable offerings.

+ €3.25 B
International revenue
since 2022

€6.9 B
Export revenue

31%
Of total revenue

+5,4%/year
Revenue generated
outside France since 2022

#3 France's Digital Trust sector is strengthening its international presence

By 2025, the share of revenue generated from exports will reach 31%, or 6.9€ billion, reflecting a slight increase in the sector's international expansion.
More broadly, revenue generated outside France is projected to grow by an average of 5.4% annually between 2022 and 2025, a sign of French players' growing foothold in European and global markets. Expansion at the European level is further facilitated by the adoption of foundational regulatory frameworks in recent years, particularly regarding artificial intelligence, trusted solutions, cybersecurity, and data protection, which help harmonize markets and create deployment opportunities for French players.
This internationalization is based on both:
- exports
- external growth strategies

Acquisitions carried out by French companies abroad, particularly in Europe, show that the sector is no longer content to simply export from France, but is increasingly seeking to build a local presence in target markets. This trend is particularly evident in the United Kingdom and more broadly across Europe, where several French groups have carried out targeted acquisitions to expand their geographic reach, customer base, and expertise. While international expansion is increasingly emerging as a driver of growth, its progress remains insufficient in the face of intense global competition, making it a strategic imperative for achieving critical mass

Against a backdrop of slowing growth, the Digital Trust sector is entering a phase of consolidation and polarization:
- Growth is becoming more challenging and is concentrated among the most differentiated players
- Value creation is shifting toward less arbitrage-prone segments related to security, compliance, and sovereignty;
- Internationalization is emerging as a key driver of competitiveness.

In this context, the impact of artificial intelligence is a defining factor for the years ahead. Its development, particularly through agent-based approaches, is likely to profoundly transform certain segments, especially consulting and services.

Furthermore, the rise of AI already appears to be reshuffling the deck when it comes to investment. It could contribute to a realignment of stakeholders' priorities and a temporary slowdown in M&A activity, a trend that will require close monitoring in the coming months.

The sector is projected to generate €34.7 billion in revenue in 2025, representing 5.4% growth, a slowdown compared to previous years but still outpacing the French economy. It generates €10.6 billion in value added and accounts for 113,600 jobs in France (plus 61,300 abroad), confirming its focus on technology-intensive activities and its role as a significant contributor to skilled employment in the country.

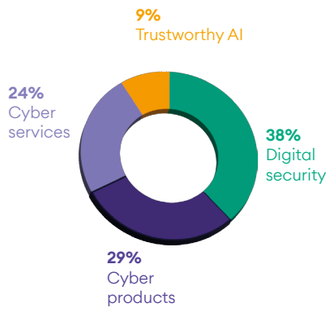
Key figures 2025

Global Revenue	**€34.7 B**
Revenue Abroad	**€12.3 B**
Revenue France	**€22.4 B**
	exported revenue incl. **€6.8 B**
Added Value France	**€ 10.6 B**

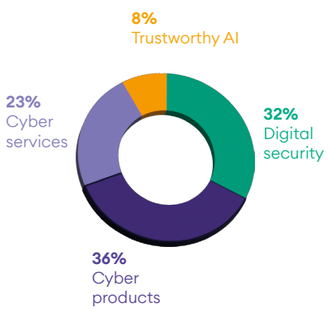
The breakdown of market segments reveals distinct patterns: digital security dominates in terms of revenue (38% of total revenue), reflecting a broad market, while cybersecurity products account for a higher proportion of companies (36%), reflecting a more fragmented ecosystem. Cybersecurity services occupy an intermediate position, particularly in terms of workforce size (27%), while trusted AI, still limited in scale (8%), is part of a trend toward gradual growth.

The main segments of digital trust in 2025

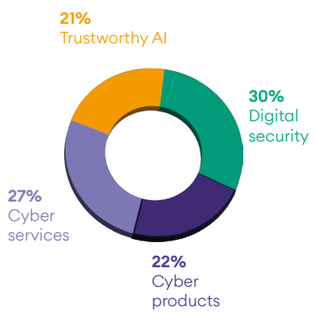
• **Revenue**



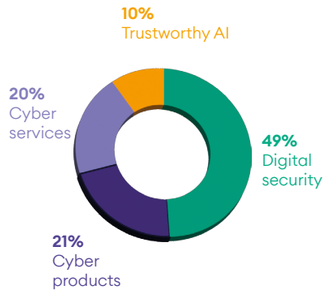
• **Number of companies**



• **Staff numbers**

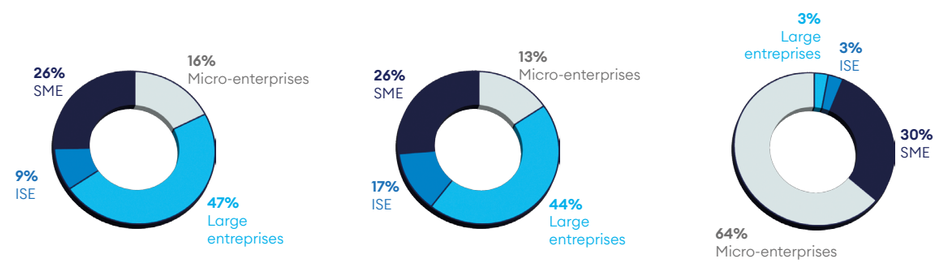


• **Added value**

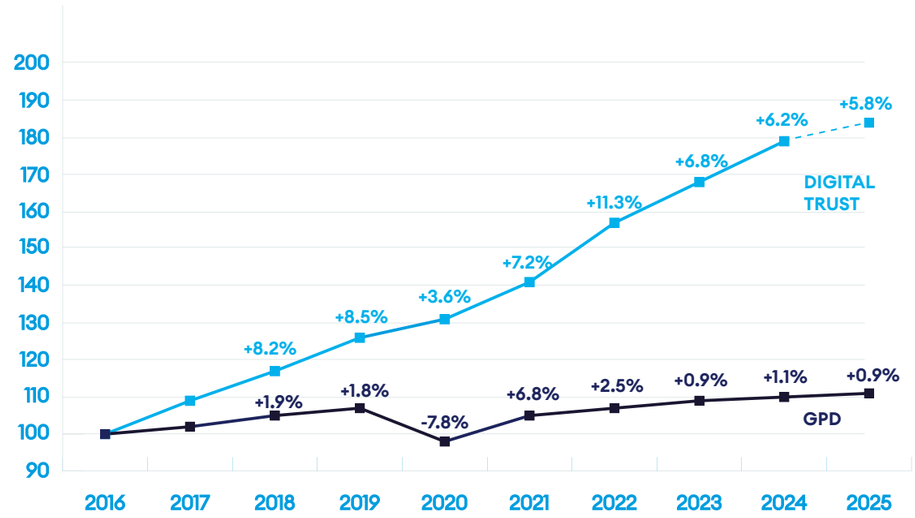


The sector is characterized by a concentration of revenue among large companies (47%), while SMEs (28%) play a significant role in value creation. The workforce is distributed almost equally between large companies (44%) and mid-sized players (SMEs and mid-sized companies, 43%). Finally, microenterprises alone account for 64% of the players, while large companies and mid-sized companies remain few in number, reflecting a fragmented economic landscape.

Breakdown by company size 2025



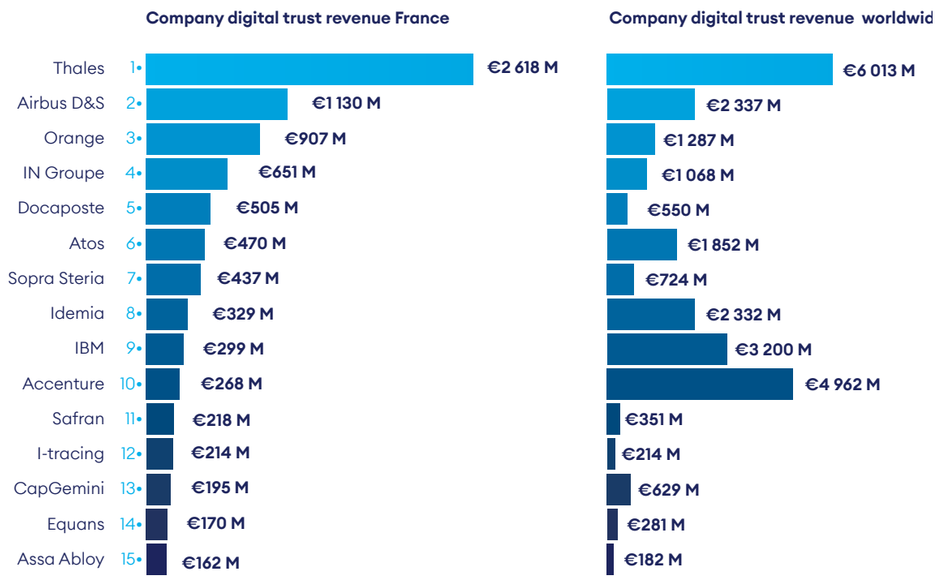
France growth comparaison 2017- 2025



Base 100 in 2016

GDP growth as measured by INSEE and the IMF in 2025.
This figure does not take into account growth in the trusted AI sector.

Top 15 players France 2025



Note: The 2026 edition of the Observatoire introduces an expanded scope of analysis with the inclusion of the Trustworthy AI segment in 2025. This structural change has led to an adjustment in the reported revenue figures for the companies concerned, affecting their ranking in the Top 15. Several groups have benefited from the integration of their Trustworthy AI activities, including Thales, Airbus, Orange, Atos, and Idemia. Additionally, certain data has been updated following the release of new financial statements from French offices, particularly for companies whose figures had not been available in previous editions, such as Orange Cyberdéfense. Finally, some Trustworthy AI activities have been reallocated from other existing segments. For all these reasons, the 2026 and 2025 results are not directly comparable to those of previous editions.

The Digital Trust sector in France enjoys European and global leaders:

- **Thales** has created a world leader in digital security with the acquisition of Gemalto in 2019, and Imperva and Tesserent in 2023.
- **Thales, Idemia, Docaposte and IN Groupe** are world leaders in digital identity, identification and authentication.
- **Airbus Defence & Space** is an European leader in digital security and a global leader in wide area observation and secure communications.
- **Atos (Eviden), Orange, Sopra Steria and Capgemini** are the 4 French leaders among digital services companies, and are also the French leaders in cybersecurity (with **Thales** and **Airbus Defence & Space**).
- **Docaposte** is a French leader in many segments of digital security and cyber products. Docaposte is the initiator of a sovereign cloud offer «Numspot», announced in the fall of 2022. In collaboration with Dassault Systèmes, Bouygues Télécom and CDC, this sovereign cloud offer will enable the operation of trusted services that are SecNumCloud certified.
- The American company **Accenture** maintains its position in the top 10 thanks to its growth and previous takeovers (Arismore, etc.)
- **Thales** includes Gemalto, Imperva, Tesserent and Ercom.
- **Atos** includes Idnomic, Ipsotek, Motiv ICT Security, Sec consult, In fidem, Paladion...
- **Orange Cyberdéfense** includes Securelink, Securedata, Lexsi...
- **Sopra Steria** includes CS Group, Tobania, Ordina, Sodifrance, Bluecarat, Kentor, Eva Group...
- **Capgemini** includes Altran et Leidos Cyber.
- **Docaposte** includes AR24, CDC Arkhineo, Open Value...
- **Accenture** includes Arismore, Link by net, Openminded...
- **Chapsvision / Flandrin** technologies includes Deveryware, Bertin IT, Vecsys, Elektron et Geotrend.

Top 1-10 players in France

THALES · AIRBUS DEFENCE & SPACE · Atos · DOCAPOSTE · IBM · IDEMIA · IN GROUPE · orange · sopra steria · accenture

Top 11-20 players in France

Digital Trust Revenue generated in France ranged between €135 M and €220 M

EQUANS · Capgemini · CHAPSVISION DATA MAKE SENSE · i-TRACING CYBERSECURITY · SAFRAN · WORLDLINE · ASSA ABLOY · exaprobe | econocom · FORTINET

Top 21-50 players in France

Digital Trust Revenue generated in France ranged between €60 M and €130 M

SPIE · WAVESTONE · SFR · CROSSCALL · squad · NAVAL GROUP · CHEOPS TECHNOLOGY · ANTEMETA · Stordata · Sogetrel · Ledger · Almond · nxo · cogelec · tessi · ALTEN · Deloitte. · EY · Linxens · SIEMENS APIXIT · CGI · Palantir · pwc · CISCO · NOKIA · TREND MICRO

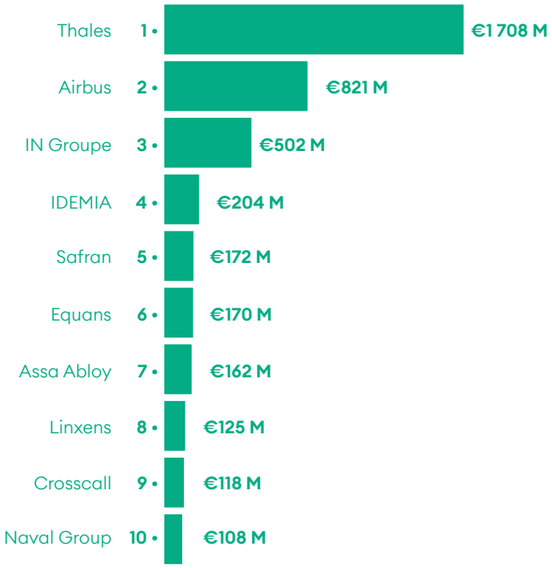
Note: Flags indicates the nationality of capital of the players in France.

Among the players ranked between 10th and 20th, and generating more than €135m in Digital Trust revenue from France in 2025, are French companies such as Capgemini, Nomios and I-Tracing in cyber services, Worldline in payment security, Safran, including specific AI activities, Equans in digital security, and ChapsVision in intelligence and information gathering, as well as cyber products resulting from its merger with Deveryware. This group also includes foreign players such as Assa Abloy in access control and authentication, Fortinet in cyber products, and Econocom in cyber services.

Companies positioned around 50th place in the sector all generate Digital Trust revenue in France of approximately €60m. These include Somfy, Securitas, through Stanley Security, Serma Safety & Security, Schneider, Honeywell, Palantir, Devoteam, SAP, Oracle, Bechtle, Inetum, Claranet, Computacenter and Scalian, among others. Finally, although French players largely dominate the sector's top 10, foreign companies established in France, particularly US companies, have a stronger presence among players ranked between 10th and 50th.

FOCUS

Digital Security Segment



• Growth 2024-2025
+2.4%

• Revenue
€8 559 M

• Workforce
34 462

• Number of companies
1 772

• Added value
€3 438 M

	Revenue M€	Workforce	Number of companies	Added alue M€
Access control	1 866	6 928	333	695
Identification & Authentification of people	2 458	9 562	509	966
Wide area observation and detection	572	2 246	191	305
Tracking and tracing	670	2 685	224	252
Secure communications	1 729	6 806	315	652
Command, control and support for decision making	793	3 346	275	367
Intelligence and information gathering	471	2 888	234	201

FOCUS

Cybersecurity Product Segment

• Growth 2024-2025
+6.4%

• Revenue
€6 502 M

• Workforce
25 433

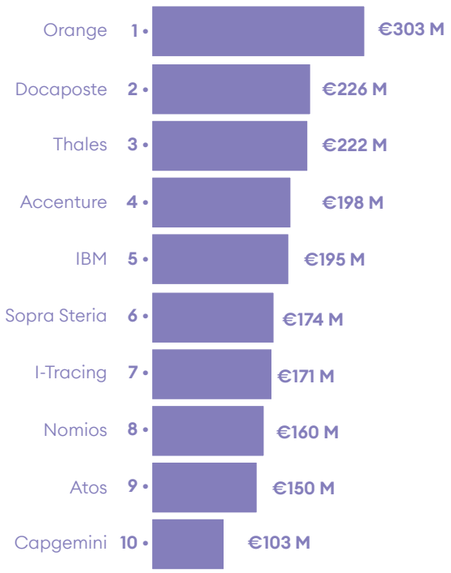
• Number of companies
749

• Added Value
€3 817 M

	Revenue M€	Workforce	Number of companies	Added Value M€
Cyber governance	1 169	5 843	233	670
Identity and access management	948	3 071	214	604
Data security	1 974	7 178	356	1 190
Application security	440	1 599	177	304
Secure digital infrastructures	1 581	6 281	360	897
Product and equipment security	390	1 480	161	152

FOCUS

Cybersecurity Services Segment



• Growth 2024-2025
+3.4%

• Revenue
€5 407 M

• Workforce
30 335

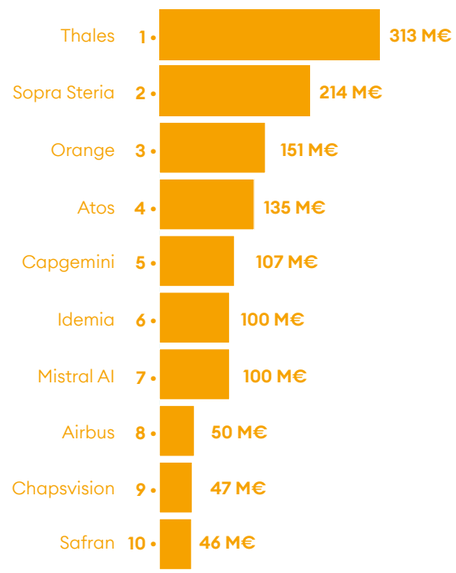
• Number of companies
730

Added Value
€2 499 M

	Reevnue M€	Workforce	Number of companies	Number of companies
Audit, planning and consulting in cybersecurity	2 366	13 711	684	971
Cyber implementation	1 742	10 348	477	755
Outsourcing - operating	1 179	5 202	367	701
Cybersecurity training	120	107	207	72

FOCUS

Trusted AI Segment



• Growth 2024-2025
+23.4%

• Revenue
€1 957 M

• Workforce
23 339

• Number of companies
379

• Added Value
€900 M

	Revenue M€	Workforce	Number of companies	Added Value M€
Generative AI	437	3080	144	201
Specific AI	1521	14 126	310	699

1. DIGITAL TRUST

1.1 Cybersecurity, Digital Security and Trustworthy AI: a complementary technological triptych
1.2 The ACN's purpose, missions and values
1.3 The Scope of Digital Trust - segmentation
1.4 Methodology

1.1 CYBERSECURITY, DIGITAL SECURITY AND TRUSTWORTHY AI: A COMPLEMENTARY TECHNOLOGICAL TRIPTYCH

Digital Trust is the foundation of digital progress. Over the years, it has become a societal and industrial concern as critical as the development of digital technologies themselves. It reflects the confidence individuals and organisations can place in digital systems–now central to all aspects of life - to enhance their physical, financial, and reputational security while protecting their privacy and data, including personal information.

The Observatory of Digital Trust covers three key industries:

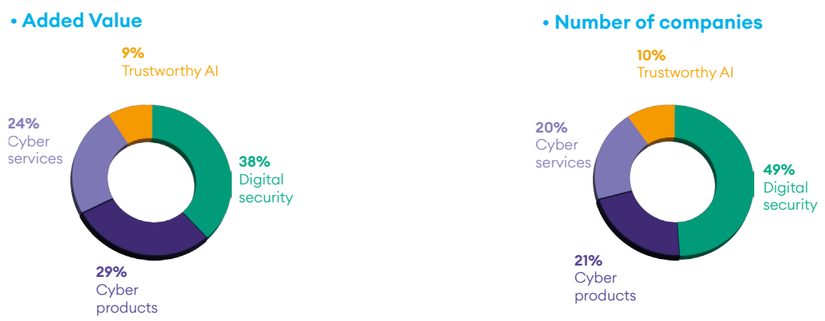
• **Cybersecurity**, which refers to the "internal" security of digital systems. It includes two categories of activities, often combined in practice: services (consulting, design, implementation, operation, training) and software & solutions. These serve professional markets (government, public sector, critical infrastructure, companies, SMEs) as well as the general public (computers, smartphones, connected homes, vehicles, and Iot devices).

• **Digital Security**, which encompasses electronic products and solutions that implement secure digital systems to establish trust in the external world. These technologies are deployed to build confidence in the citizen environment–particularly through identity and access management, biometrics, secure transactions, connected objects and vehicles, industrial processes, logistics, transportation, networks, and smart cities.

Digital security products include hardware (smart cards, identity documents, readers) and equipment (access control, biometrics, detection, geolocation, etc.).

• **Trustworthy AI**, which refers to artificial intelligence designed and deployed according to stringent legal, technical, and ethical standards. It is based on principles such as transparency, explainability, robustness, safety, human oversight, and respect for privacy. It also includes a sovereignty dimension, focusing on solutions developed by French providers. Trustworthy AI includes both generative models (LLMs, SLMs, GAI, etc.) used to generate content or assist users (chatbots, recommendation engines, summarisation tools), and domain-specific models tailored to targeted use cases (information extraction, image or voice processing, fraud detection, predictive maintenance, cybersecurity, etc.) depending on industry needs and data types.

Turnover and number of companies in 2025

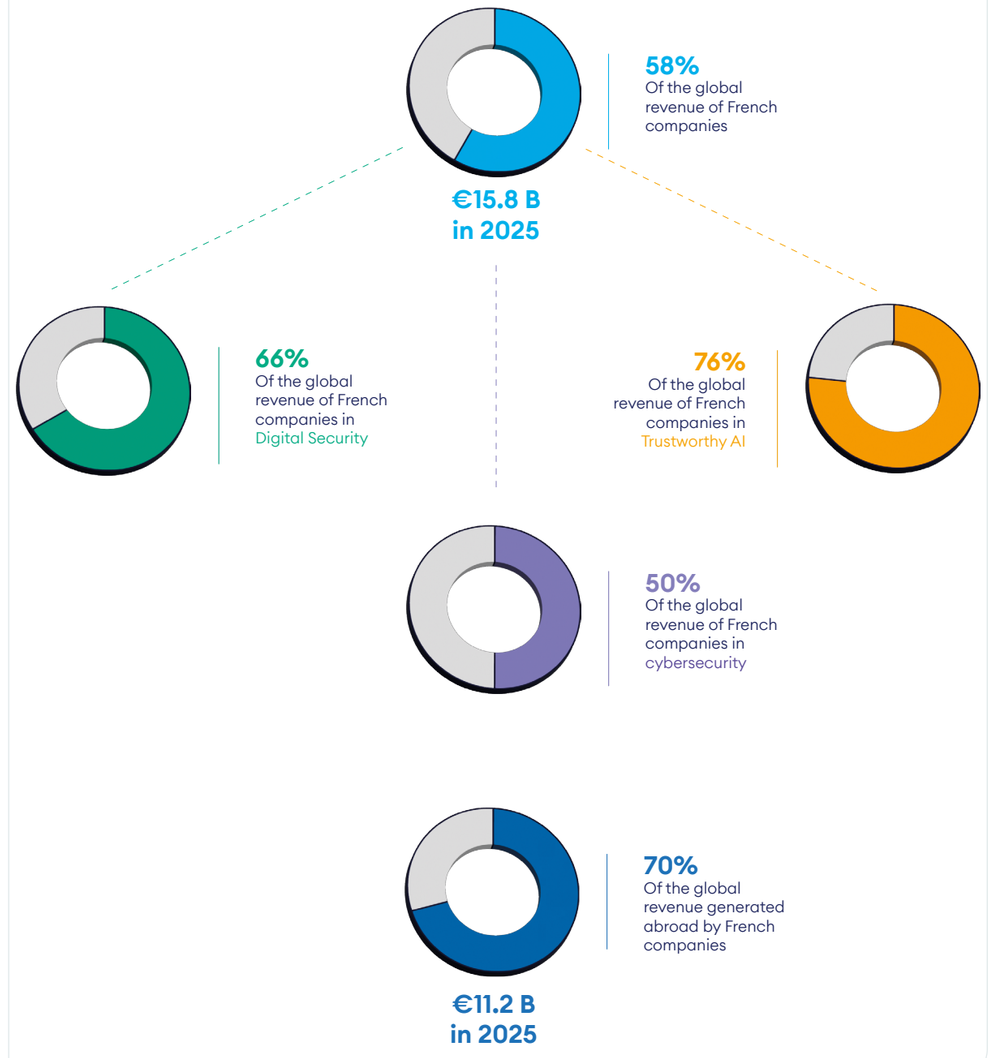


ACN is at the core of the industry

Among the ACN members there are:

• **10 large companies or ISE, including the 9 French leaders in Digital Trust.**
• But also **76 SMEs, micro-enterprises** and **innovative start-ups as direct members** and more than **200 SMEs in the sector** via the ecosystems of its partner members (SPAC, GICAT, Bretagne Next, etc).

ACN members account for:



1.2 THE ACN'S PURPOSE, MISSION AND VALUES

"To shape our digital future, the Alliance for Digital Trust inspires, unites, strengthens, and takes action on behalf of businesses and society."

The Alliance for Digital Trust (ACN) is a professional union representing French companies in the digital trust sector, focusing on digital identity, cybersecurity, trusted artificial intelligence, blockchain, and trusted infrastructure. The ACN's missions are organized around five strategic priorities.

- **Inspiring and informing public policy decisions:** ACN is committed to advancing a strategic vision of digital trust in the service of sovereignty and the public interest. As such, it represents the sector before public authorities in France and Europe, while contributing to national and European legislative and regulatory debates.
- **Serving as a source of proposals for the sector:** ACN contributes to public debates through analysis, innovation, and foresight. It produces reference documents, such as roadmaps, white papers, and common positions, and formulates concrete proposals on laws, regulations, and public policies.
- **Acting to advance the sector's development and impact:** ACN leads collective initiatives to serve its members and the sector, supports the emergence of trusted French digital solutions, and facilitates operational initiatives with tangible impact.
- **Strengthening the sector's sovereignty and competitiveness:** ACN works to increase the competitiveness and influence of the French sector, while promoting trustworthy, sustainable, and responsible digital technologies.
- **Bringing together and structuring the ecosystem:** ACN unites stakeholders around a shared vision and common goals by shaping the sector's momentum and coordinating initiatives, while fostering cooperation among companies, institutions, academic bodies, and European partners.

ACN's values are based on five fundamental pillars:

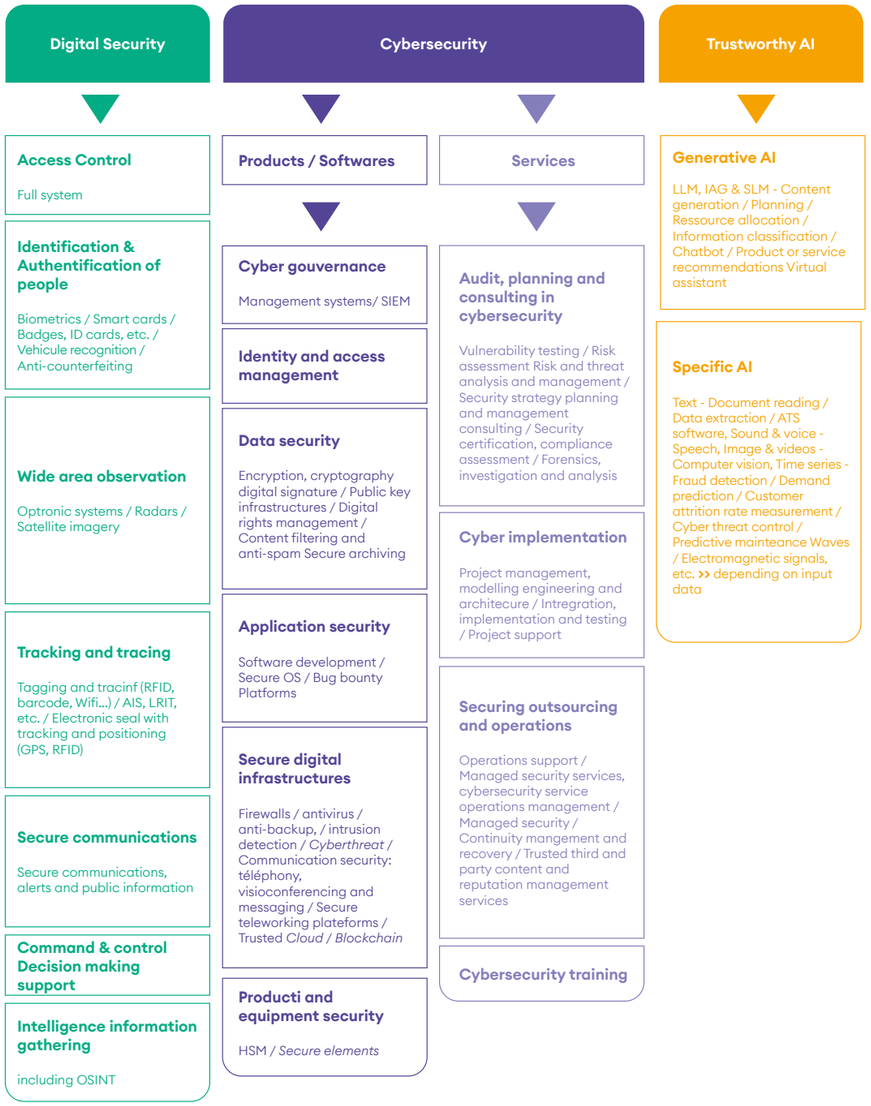
- **Collectivity** is at the heart of ACN's DNA. ACN believes in the power of collective intelligence, the diversity of perspectives, and the pooling of expertise. This value is reflected in the unification of industry stakeholders, the development of shared positions, and the pursuit of the common good beyond individual interests.
- **Responsibility** is another key value of ACN. This responsibility entails an ethical, sustainable, and sovereign approach to technology : managing dependencies, complying with regulatory frameworks, protecting data, and considering the long-term consequences of technological choices. Being responsible means anticipating, guiding, and taking ownership of decisions made in the public interest.
- **Trust** is a prerequisite for any sustainable cooperation. ACN is committed to creating a framework for transparent, fair, and rigorous dialogue among its members, partners, and institutions. This trust is based on the credibility of the positions defended, the rigor of the work carried out, and the consistency of commitments, in order to build solid and lasting relationships.
- **Cooperation** goes beyond simple networking ; ACN fosters concrete working relationships between public and private actors, large companies, SMEs, startups, and the academic and institutional sectors. This value is reflected in the desire to co-create solutions, pool efforts, and move beyond siloed thinking to collectively strengthen the digital sector.
- **Action** is at the heart of ACN's identity and credibility. It reflects the commitment to move from vision to implementation and to transform collective efforts into concrete, useful results for the sector. This value is embodied in operational actions, market development, the structuring of offerings, support for stakeholders, and contributions to digital sovereignty. For ACN, taking action means committing responsibly, with high standards, pragmatism, and a long-term perspective, so that every action sustainably strengthens the trust, competitiveness, and strategic autonomy of the French digital ecosystem.

1.3 THE SCOPE OF DIGITAL TRUST: SEGMENTATION

The diagram below shows the different segments of the Digital Trust, divided into three areas:

- **Digital security**, which corresponds to trusted electronic systems or subsystems;
- **Cybersecurity products**, which corresponds to the development of cybersecurity software;
- **Cybersecurity services**, which corresponds to auditing, consulting, and implementation of cyber products, secure outsourcing or cyber training.
- **Trustworthy AI**, corresponding to generative AI or specific AI developed in France according to trust criteria.

Scope of digital Trust



1.4 METHODOLOGY

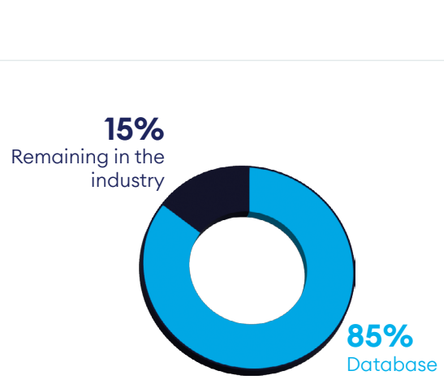
The aim of the Digital Trust Sector Observatory is both to define the scope of the sector and to assess its economic significance and characteristics.

The data presented in this report is drawn from a DECISION database covering 1,010 companies out of the 2,573 that make up the Digital Trust sector. This database includes:

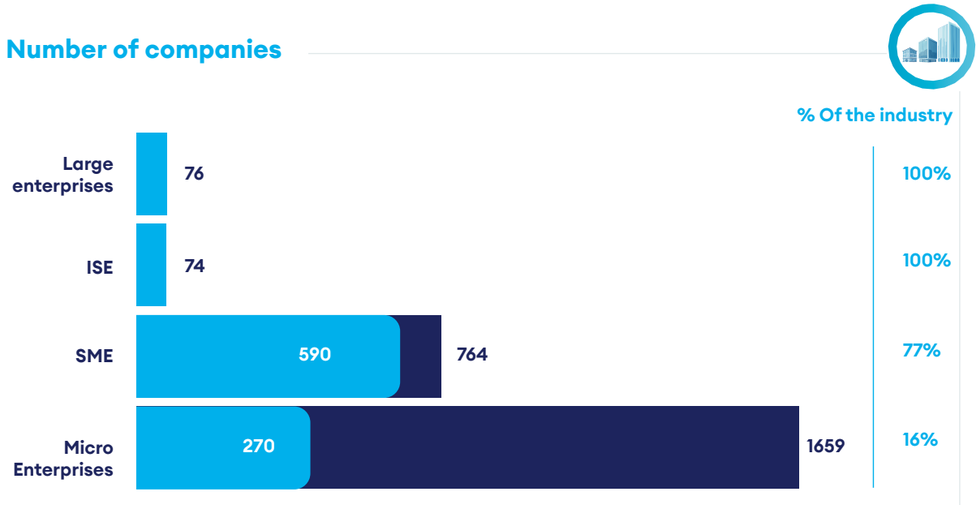
- All large companies in the sector (76/76);
- All medium-sized companies (ETI) in the sector (72/72);
- The majority of small and medium-sized enterprises (SMEs) in the sector (590/764);
- The most notable and innovative micro-enterprises (TPE) and start-ups (270/1,659).

Thus, although only 39% of the sector's companies are included in the database, it is representative of 85% of the total turnover of the Digital Trust sector in France.

Revenue



Number of companies



Data gathering for the database

For each company in the database, the following data are collected annually for France:

• **Administrative data:** SIREN, SIRET, address, NAF code, name of the main shareholder of the group, date of creation, name and function of the manager, contact details, etc...

• **Economic data for the period 2015-2025:** Revenue, number of employees, export revenue, added value, net profit.

Player analysis and segmentation

DECISION then carries out a specific analysis of each company in order to estimate the share of the activity dedicated to digital trust and the distribution of the revenue according to the 19 ACN segments (the ACN segmentation is now fully integrated in the wider segmentation of the Comité Stratégique de la Filière des Industries de Sécurité). This analysis of companies is carried out thanks to DECISION's expertise in the security sector acquired over the last 10 years, and in particular thanks to direct interviews with the key players in the sector. Finally, an online form is sent every year to the members of the sector and allows to refine the analyses.
From the information in the database, a method of extrapolation has been implemented in order to construct figures for the entire industry in France.

Growth calculation

Growth in France is estimated each year for each of the segments by taking into account three components:

• **Database:** A sub-sample analysis is carried out in order to measure the total growth in France of representative players in each segment, i.e. companies generating more than 10% of their revenue from their activities in the segment concerned.

• **Company documents:** Analysis of annual reports, financial documents and communications from companies in the sector.

• **Online questionnaire:** The online questionnaire filled in each year by the industry members provides data on the growth of the past year. For the 2026 edition, the members who answered the questionnaire represent 12% of the sector's revenue in France.

Comparisons with previous Observatories

Each year, in addition to estimating growth, DECISION refines the segmentation of the various players in the sector, in particular thanks to information from the online questionnaire.

Consequently, **the figures in absolute value of each edition of the Observatory are not directly comparable**. The figures of this Observatory are presented for the year 2024 and according to the new segmentation of the actors. The updated 2023 figures are presented later in the following sections of this report.

2. AN IMPORTANT AND DYNAMIC INDUSTRY

2.1 The French sector with the strongest growth over the period 2016–2024
2.2 Digital Trust is the industrial sector whose activity creates the most wealth in France
2.3 Digital Trust is a fully-fledged french industrial secteur
2.4 French players are at the top level in terms of skills and R&D
2.5 The growth in Digital Trust is part of a global dynamic
2.6 Growing competition from foreign players
2.7 A sector with great potential if the right strategic choices are made

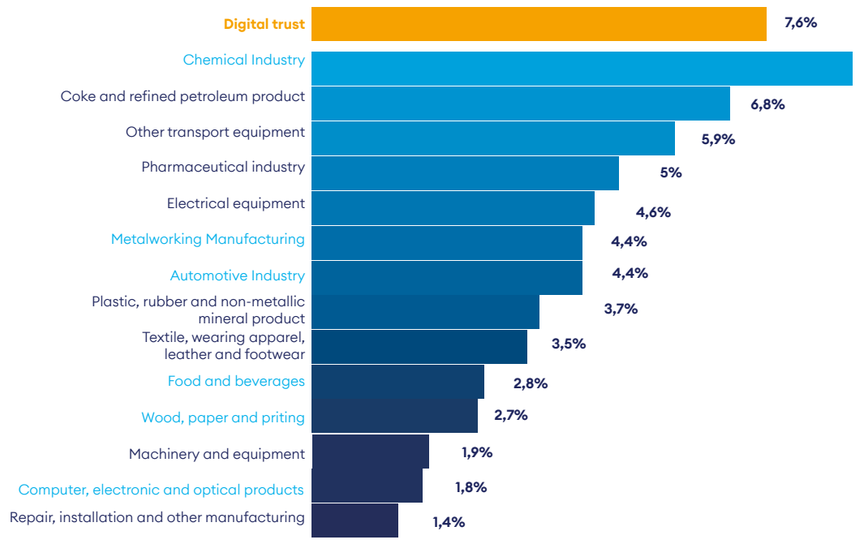
2.1 THE FRENCH SECTOR WITH THE STRONGEST GROWTH OVER THE PERIOD 2016–2024

Over the period 2016–2024, Digital Trust stands as the fastest-growing industrial sector in France, with an average annual growth rate of 7.4%. Although measured using a method that is not directly comparable, the only other French industrial sectors recording growth above 5% are the textile and clothing industry, the pharmaceutical industry, the chemical industry, and the agri-food industry. Other industries recorded average annual growth rates of between 0% and 5% over the same period.

Digital Trust is also one of only four sectors, out of a total of fifteen, that did not experience a recession in 2020. With growth of 3.6% that year, it was the sector that proved most resilient to the COVID crisis and its consequences.

This resilience reflects sustained demand for Digital Trust goods and services. As a result, by 2030, Digital Trust could become the 12th largest French industrial sector out of fifteen in terms of value added, overtaking the electrical equipment sector.

Average annual growth of french industries over the 2016-2024 period



KEY

---- Industries that have both a dedicated Eurostat segment and strategic committee in the Conseil National de l'Industrie (CNI)

---- Industries that have a Eurostat segment and wich corresponds to some extent to industries with a strategic committee in the CNI (to be treated case by case)

* **Source:** DECISION, Observatory of Digital Trust

Source: DECISION, based on Eurostat data from 2016 to 2024

2.2 DIGITAL TRUST IS THE INDUSTRIAL SECTOR WHOSE ACTIVITY CREATES THE MOST WEALTH IN FRANCE

Digital Trust is the most productive sector with an added valut rate of 48% (Added Value / Revenue). In other words, Digital Trust is the industrial sector with the highest degree of wealth creation, i.e. transformation of products during the activity. Thus, the increase in revenue in this sector results on average in a higher rate of transforming activity on French soil compared to other French industrial sectors.

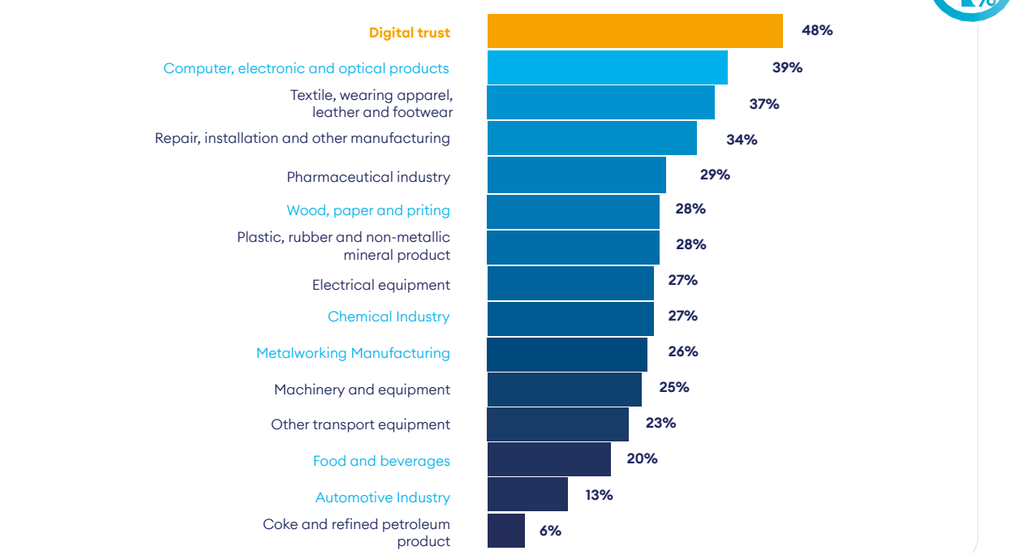
This phenomenon is mainly explained by three factors:

1. **The percentage of activity dedicated to services is relatively high in the French Digital Trust sector** (24% in 2025), through cybersecurity services (consulting, auditing, training, etc.). By definition, service activities have a very high added value rate because they use very little intermediate consumption and correspond almost exclusively to the transformation of products during the activity. However, this phenomenon alone does not justify the French security industry being the leader in terms of value added rate, as most of the French industrial sectors also include a significant part of services.

2. Electronic products dedicated to Digital Trust (digital security) correspond to 38% of the total revenue of the Digital Trust sector. However, while for the French electronics industry as a whole, a large part of the production stages upstream of the value chain is carried out in Asia, **this phenomenon hardly applies to the Digital Trust segment, which maintains all the production stages in France as much as possible because of its proximity to the sovereign sectors.** Other French sectors focus more strongly on integration activities upstream of the value chain and on pure engineering activities (design, development, etc.). As a large part of the value chain of the digital security industry is carried out from France, the rate of value added increases.

3. Finally, cybersecurity products account for 29% of the total revenue of the security industry and involve **a very large proportion of highly qualified jobs** (software development, etc.), associated with a very high rate of added value (at levels close to those of cybersecurity services).

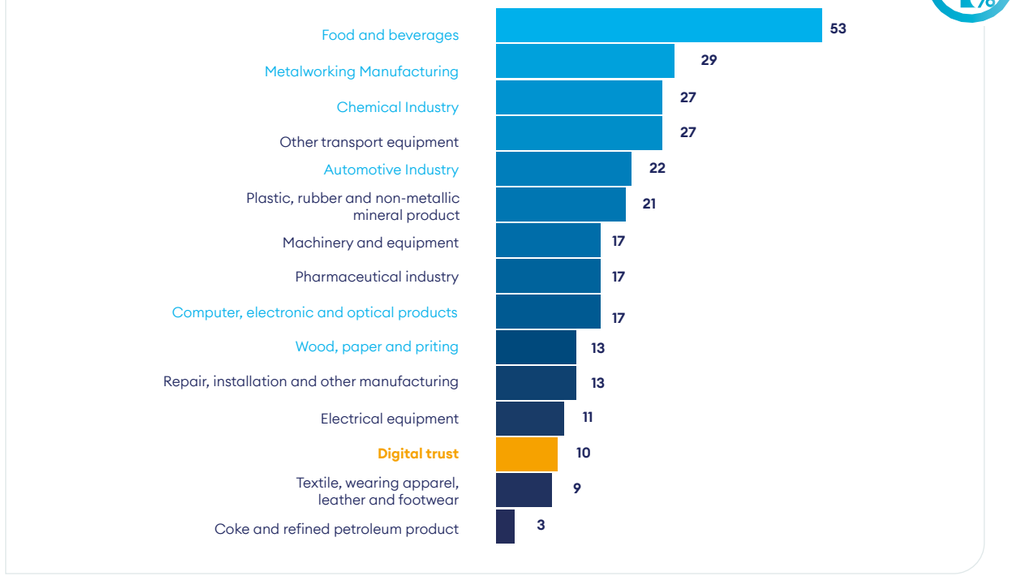
Value-added to turnover ratio (VA/Turnover) of French industries in 2023



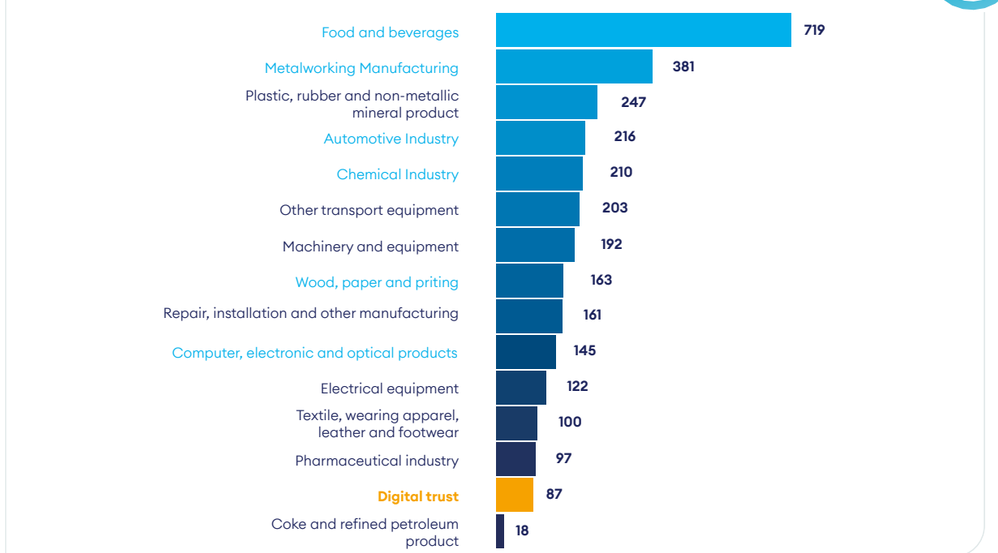
2.3 DIGITAL TRUST IS A FULLY-FLEDGED FRENCH INDUSTRIAL SECTOR

Digital Trust is an industrial sector in its own right. In terms of added value, it is close to the textile and clothing sector and electrical equipment sector. In terms of employment, it is much larger than the coke and refined petroleum sector and is close to the pharmaceutical industry.

Added Values of french industries in 2023 (€ Billion)



Worforce in french industries in 2023 (in thousand)



Source : DECISION, Eurostat, OCDE

2.4 FRENCH PLAYERS ARE AT THE TOP LEVEL IN TERMS OF SKILLS AND R&D

Thanks in particular to French excellence in research and development, the vast majority of French Digital Trust companies are positioned in the high-end segments of their markets, offering solutions at the cutting edge of what technology currently makes possible. France excels in particular in the following areas:

• **Artificial Intelligence & Machine learning:** France excels in deep learning. For several years, GAFAM companies have established research centres dedicated to this field and have been actively recruiting French talent. France is also seeing the emergence of leading players in generative AI, such as Mistral AI, which has become a French unicorn. In the field of specialised AI, France benefits from a broad ecosystem offering business-specific solutions across various markets, including healthcare, insurance and logistics.
On the public R&D side, INRIA notably has teams dedicated to defence and attack strategies based on deep learning.

• **Cryptography:** France has historically been one of the world leaders and continues to maintain its position.

• **Post-quantum technologies (including cryptography):** France remains among the world's top three countries. Within the next few years, quantum computers are expected to reach operational stages. Post-quantum cryptography is therefore one of the most critical research topics for France.

France is also well positioned in blockchain and in securing connected objects. However, public research suffers from a lack of personnel dedicated to Big Data. France has nearly 1,000 full-time academic researchers working on cybersecurity topics, particularly on the Rennes, Paris-Saclay, Brest, Grenoble and Lyon campuses. Brest, Grenoble and Lyon campuses.

2.5 THE GROWTH IN DIGITAL TRUST IS PART OF A GLOBAL DYNAMIC

At the global level, the growth of Digital Trust is driven by four factors, the first three of which are not specific to France:

1. Miniaturisation along with the falling cost of electronic components. This long-term trend makes it possible to integrate electronic security equipment on a large scale and therefore contributes to strong volume growth in electronic security equipment. In the short term, growth in electronic components is cyclical, and the 2020–2022 period was instead marked by a sharp increase in semiconductor prices. Since the beginning of 2023, the decline in semiconductor prices has resumed.

2. Digital transformation. Accelerated by the COVID crisis in 2020, companies and public administrations around the world are digitalising their processes, deploying cloud solutions and interconnecting data networks.

3. The growth from emerging countries, led by China. China notably aims to become a global leader in semiconductor production and innovation in the near future.

4. Finally, numerous technological innovations specific to the Digital Trust sector, in which France is often very well positioned both in terms of industrial players and scientific expertise: behavioural biometrics, innovations associated with secure elements, quantum computers, cryptographic developments, real-time analysis of wide-area observation data, artificial intelligence, blockchain, and others.

France has historically benefited from a powerful defence and security sector with strong export capabilities compared with the international average. It has also been able to leverage its excellence in research and development to take advantage of these four global trends and build a solid Digital Trust industry.

However, growth remains even stronger in the US and, above all, Chinese Digital Trust industries.

2.6 GROWING COMPETITION FROM FOREIGN PLAYERS

French players generate 73% of Digital Trust revenue in France, equivalent to €16.3 billion in 2025. In other words, foreign players in the sector generate 27% of the sector's revenue in France, or approximately €6 billion in 2025. This figure corresponds solely to the revenue generated by subsidiaries of foreign players in France and does not include exports by foreign players to France, which are not measured in this observatory.

Although the share of wealth generated in France by French players remains relatively high, it has been steadily declining from 2013 to 2025, and this trend is expected to continue. In particular, recent years have seen the development of US players in France, notably through the establishment of new French headquarters: Microsoft, Dell, Palantir, DocuSign, AWS, Google, Cisco, Check Point Systems, CrowdStrike International, Juniper Networks, Nutanix, F5 Networks, Palo Alto Networks, Rubrik, Okta, Netskope, Forescout Technologies, Aruba, Tufin Software, Quest Software, Proofpoint, and others. Chinese players are also expanding, with recent high-level offerings capable of competing technically with French solutions.

As with production in France, the weight of foreign players on the French market is significant, estimated at around 40%. In other words, the domestic market remains heavily influenced by foreign and non-European solutions, even though the French sector has offerings across all segments and includes technological leaders, as well as many players already large enough to cover at least the entire national market..

Significant acquisitions of French companies by foreign players took place across most segments of the Digital Trust sector over the 2013–2021 period. These include the acquisition of Arismore by Accenture in the United States, DenyAll by Rohde & Schwarz Cybersecurity in Germany, and Oberthur Technologies, acquired by the US fund Advent in 2011, followed by Safran Morpho, acquired by Advent in 2018 and merged with Oberthur Technologies under the Idemia brand in 2018. Since 2021, however, the number and size of such acquisitions have tended to decline. As a result, the only significant acquisition of a French company by a foreign company identified was that of Akka Technologies by the Swiss group Adecco in 2022.

Nevertheless, a few smaller targeted acquisitions have been observed, such as Hornetsecurity, a German company backed by US capital and acquired by Proofpoint, which acquired two French companies specialising in email security, Vade and Altospam, within the space of a year.

Above all, many players in the Digital Trust sector highlight the damaging lack of a culture of purchasing French products, both among companies and public administrations. His lack of a purchasing culture in favour of French products has naturally led French companies and administrations to turn to foreign offerings..

In a broader context of stagnant growth, with French GDP growing by 1.1% per year over the 2018–2025 period, inflation and budgetary austerity in public services, price often proves to be the primary purchasing criterion. On this criterion alone, US and Chinese players are often more competitive than French players, notably due to greater economies of scale and greater reliance on subcontracting in low-wage countries.

Beyond penalising French players in the sector, the purchase of uncontrolled foreign solutions may threaten France's sovereignty when buyers are public bodies, Operators of Vital Importance, or Operators of Essential Services.

Despite the recent awareness of sovereignty and strategic autonomy issues, the lack of a culture of purchasing French products remains particularly evident in the public sector and among major French companies.

The triptych of standardisation, certification and prescription, notably promoted by ANSSI, helps guarantee the use of reliable and secure solutions, while shifting competition away from price alone and towards technical excellence, thereby naturally favouring French players.

2.7 A SECTOR WITH GREAT POTENTIAL IF THE RIGHT STRATEGIC CHOICES ARE MADE

Digital Trust is a strategic industry because:

- The **growth** is sustainably higher than that of any other French industry;
- Digital Trust is already of **significant size;**
- French players are at the forefront in terms of **skills and R&D;**
- This sector is essential to **national digital sovereignty** and **Europea, strategic autonomy;**
- The growth potential risks being under-exploited due to **strong international competition,** particularly from China and the United States.

The conditions are in place for the leverage to be achieved if a proactive industrial policy is put in place to generate a maximum return on investment, both in terms of employment and added value on French soil and internationally.

3. KEY FIGURES OF THE INDUSTRY

3.1 Size and growth

3.2 Number of companies

3.3 Jobs

3.4 Added value

3.5 Mergers and acquisitions

3.6 A slowdown in investment in 2024, which is set to continue into 2025

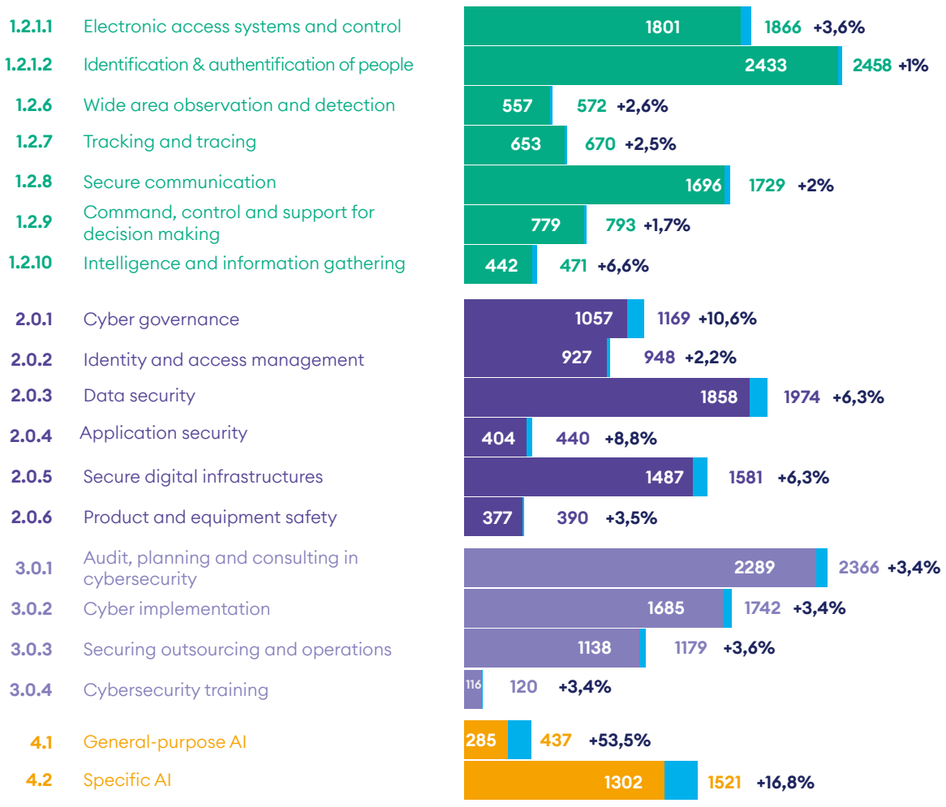
- Point of view: European Cybersecurity Investment Barometer

3.7 Strengthening SMEs and trends in the development of the start-up ecosystem

- Focus: Public funding for innovative projects in the sector - F.INITIATIVES
- Point of view: Abbas Djobo's point of view

3.1 SIZE AND GROWTH

Revenue per segment in Digital Trust : €22.42 B in 2025

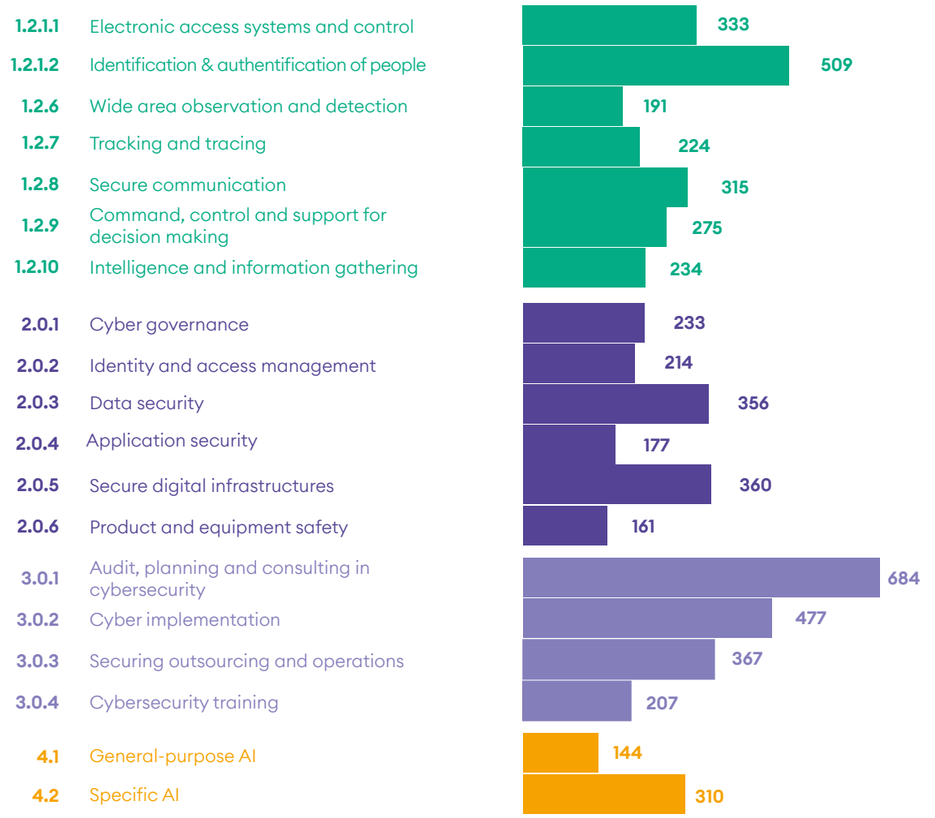


Digital Security	Cyber products & softwares	Cyber Services	Trustworthy AI
€8 559 M of revenue	€6 512 M of revenue	€5 459 M of revenue	€1 957 M of revenue
+2,4% in 2025	+6,4% in 2025	+3,4% in 2025	+23,4% in 2025

€22 425 M revenue
of digital trust in France
+5,4% in 2025

Source : DECISION Études & Conseil

3.2 NUMBER OF COMPANIES

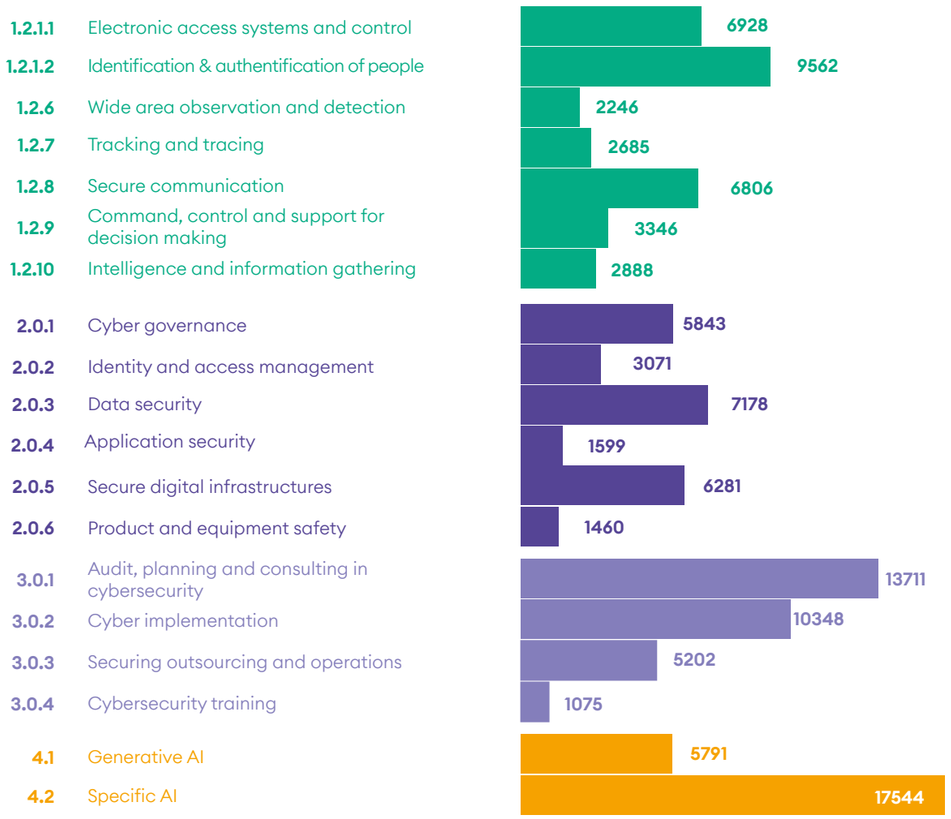


Digital security	Cyber products & softwares	Cyber services	Trustworthy AI
1 772 companies	749 companies	730 companies	379 companies

2 572 companies
in digital trust in France

Source : DECISION Études & Conseil

3.3 JOBS

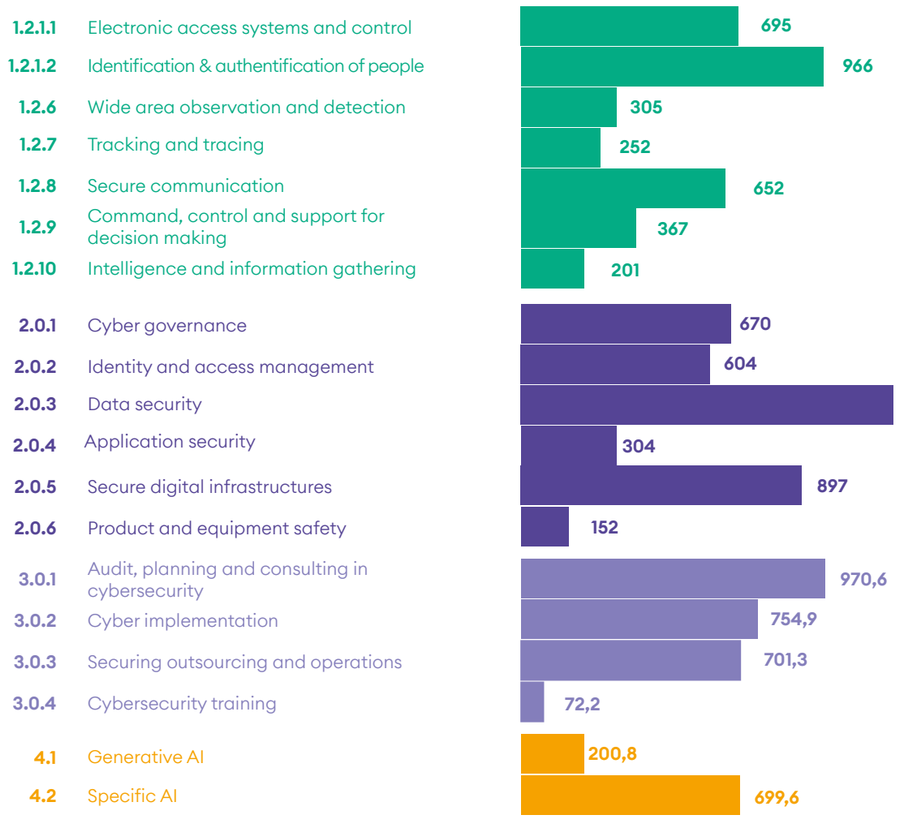


Digital security	Cyber products & softwares	Cyber services	Trustworthy AI
34 462 jobs	**25 433** jobs	**30 335** jobs	**23 339** jobs

113 600 jobs
in digital trust in France

Source : DECISION Études & Conseil

3.4 ADDED VALUE



Digital security	Cyber products & softwares	Cyber services	Trustworthy AI
€3 438 M added value	**€3 817 M** added value	**€2 499 M** added value	**€900 M** added value

€10 654 M added value
in digital trust in France

Source : DECISION Études & Conseil

3.5 MERGERS AND ACQUISITIONS

Between January 2024 and March 2026, 33 acquisitions involving companies headquartered in France were identified in the Digital Trust sector, representing an average of 15 acquisitions per year. These transactions include acquisitions between companies, acquisitions by financial funds, and transactions between funds.

Of these 33 transactions:

- 16 involved the acquisition of French companies by other French companies, representing 49%;
- 9 involved the acquisition of foreign companies by French companies, representing 27%;
- 8 involved the acquisition of French companies by foreign companies, representing 24%.

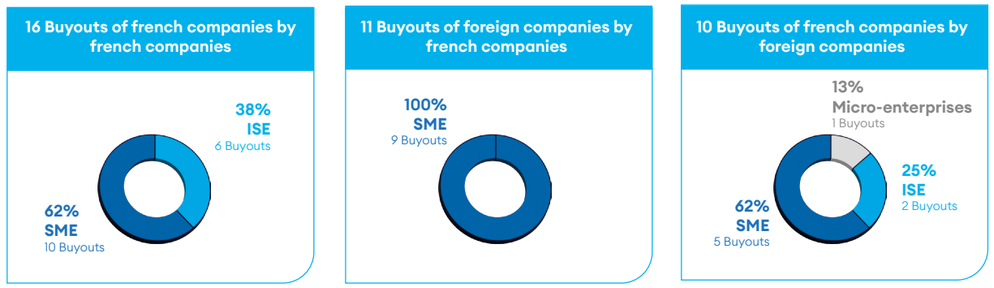
The vast majority of the companies acquired were SMEs, accounting for 73% of the total, confirming buyers' interest in growing structures. Compared with the 2017–2020 period, the frequency of acquisitions remains broadly comparable, but the average size of the target companies is smaller.

The years 2024 and 2025 stand out for their lower transaction volume, with 14 to 15 transactions recorded over these years, below the annual average observed over the 2020–2023 period, which stood at around 20 transactions per year. This decline reflects a broader economic environment that has been less favourable to mergers and acquisitions..

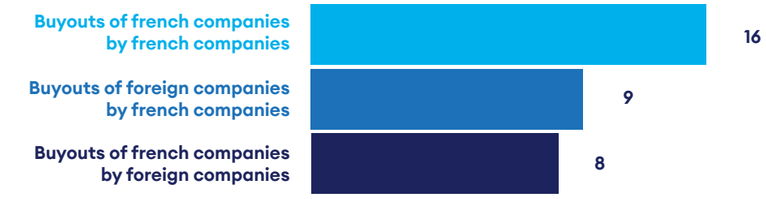
Over the recent period, M&A flows between France and foreign markets have tended to become more balanced. While the 2017–2020 period was marked by a clear dominance of acquisitions of French companies by foreign capital, this asymmetry now appears less pronounced, due to the intensification of acquisitions carried out by French players in Europe and internationally.
Nevertheless, the United States continues to play a central role in transactions involving French cybersecurity companies.

This is illustrated in particular by the acquisition of Expert Lines by Neverhack, a French company that came under the majority control of the US fund Carlyle at the end of 2023, as well as by the acquisitions of PingCastle by Netwrix and Secure-IC by Cadence. These were complemented by the transactions carried out by Hornetsecurity involving Vade Security and then Altospam.

The 33 acquisition movements are summarised in the diagram below.



Overview: companies takeovers over the period 2024-2026



1• Main acquisitions since 2024 from the French Digital Trust leaders

Airbus Defence and Space strengthens its cyber sovereignty strategy with the announced acquisition of Ultra Cyber

In March 2026, Airbus Defence and Space announced the signing of a definitive agreement to acquire Ultra Cyber Ltd from Cobham Ultra. This transaction forms part of a broader strategy aimed at maintaining Airbus as a leading European player in multi-sovereign cybersecurity, while consolidating its position as a trusted partner of the United Kingdom and its allies.

With more than 200 employees, mainly based in Maidenhead, Ultra Cyber brings Airbus sovereign cyber capabilities that complement those already developed in the United Kingdom, notably in Newport, Wales.

The transaction also strengthens the group's end-to-end cyber portfolio, while adding specialised expertise in airborne data links, in connection with Airbus' military activities.

Following the acquisition of Infodas in Germany in 2024, this new step confirms Airbus' ambition to structure a pan-European cyber business covering several key national markets.

It should be noted, however, that completion of the transaction remains subject to customary regulatory approvals and is not expected until the second half of 2026.

IN Groupe finalises the strategic acquisition of IDEMIA Smart Identity and positions itself among the sector's top five players

Following the opening of exclusive negotiations in September 2024, IN Groupe finalised the acquisition of IDEMIA Smart Identity on 1 July 2025.

This transaction represents a major step change for the group, which is now targeting nearly €1 billion in revenue and around 4,000 employees worldwide.

It simultaneously strengthens its positions in physical identity, digital identity and trust services, while expanding its international footprint.

Beyond the critical mass achieved, the transaction also consolidates key technological capabilities in secure credentials, software and identity solutions, in a context where sovereignty, cybersecurity and regulatory compliance issues are becoming increasingly important.

Orange Cyberdefense consolidates its European presence with the targeted acquisition of ensec in Switzerland

With the acquisition of ensec, finalised in July 2025, Orange Cyberdefense continued to strengthen its geographical and operational footprint in a strategic European market. This transaction enables Orange's cyber subsidiary to acquire a recognised Swiss player in consulting, security integration and managed security services, while reinforcing its presence in a country characterised by strong local demand, high regulatory requirements and heightened sensitivity to digital trust issues. The integration of around 40 additional experts brings the number of Orange Cyberdefense specialists in Switzerland to nearly 140.

Ekinops strengthens its European positioning in SASE

In 2025 and 2026, Ekinops pursued an external growth strategy to position itself as a leading European player in the network cybersecurity market.

The acquisition of Olfeo, finalised at the end of May 2025, enabled the group to integrate a French software publisher specialised in SSE, or Security Service Edge.

This transaction strengthened Ekinops' capabilities in securing web and cloud access, while positioning it in the fast-growing SSE and SASE segments. Following this first acquisition, Ekinops announced in March 2026 the acquisition of Chimere, a French specialist in universal ZTNA, or Zero Trust Network Access.

This second transaction complements the group's technology portfolio and accelerates the execution of its strategic plan to offer an integrated solution combining SD-WAN, SSE and ZTNA.
Through these two acquisitions, Ekinops is seeking to build a sovereign European access cybersecurity offering capable of meeting the growing needs of companies and operators in terms of secure connectivity, compliance and simplified deployment.

The United Kingdom appears to be the most attractive foreign market for French acquirers

The transactions identified show the particular attractiveness of the United Kingdom for French companies. Since 2024, five acquisitions of British targets or companies established in the UK have been launched: Bridewell by I-Tracing, Dionach by Nomios, MetaCompliance by Keensight Capital, Intragen by Nomios, and the acquisition of Ultra Cyber announced by Airbus Defence and Space in March 2026. These transactions cover a range of varied and complementary areas of expertise, from strategic cybersecurity consulting to identity management, penetration testing, human risk awareness and sovereign cyber capabilities linked to defence.

2•The main acquisition of French companies by foreign investors

US capital remains central to transactions involving French companies

US players remain highly active in acquisitions of French companies in the sector. The most notable examples include the acquisition of Expert Lines by Neverhack, a French group that came under the majority control of Carlyle; the acquisition of PingCastle by Netwrix; and the acquisition of Secure-IC by Cadence.

These transactions concern varied but strategic segments, ranging from cyber services and security audits of Active Directory environments to embedded cybersecurity and security IP.

The acquisition of Vade Security by Hornetsecurity in 2024, followed by the acquisition of Altospam by the same group in 2025, initially strengthened Hornetsecurity's French footprint in email security.

However, the transaction took on an additional dimension with the acquisition of Hornetsecurity by Proofpoint, finalised in December 2025.

This point is particularly notable given that Vade had previously been involved in major litigation with Proofpoint in the United States over intellectual property and trade secret issues.

CGI acquires Apside and strengthens its technological and sectoral base in France

The acquisition of Apside by Canada-based CGI, finalised in August 2025, also illustrates the interest of large foreign players in French companies with critical mass and differentiated technological expertise.

With more than 2,500 employees, including 2,200 in France, Apside enables CGI to consolidate its presence in the French market and strengthen its capabilities in several strategic areas, including data, artificial intelligence, cloud and cybersecurity.

3.6 A SLOWDOWN IN INVESTMENT IN 2024, CONFIRMED IN 2025

As it does every year, DECISION draws on Tikehau Ace Capital's European Cybersecurity Investment Barometer, supplementing it with its own research to take account of the specific segmentation of the ACN, which encompasses all digital security activities beyond cybersecurity.

Following the peak observed in 2023, fundraising by French Digital Trust start-ups slowed over the last two years. The total amount raised fell from €456m across 41 deals in 2023 to €352m across 27 deals in 2024, and then to €274m across 24 deals in 2025. The contraction observed in 2024 therefore continued in 2025. The beginning of 2026 remains too partial to identify an underlying trend, with €66m raised across 4 deals between January and March, but it shows that significant funding rounds are still taking place.

This dynamic also remains driven by a small number of structuring deals. In 2023, Ledger and ChapsVision alone accounted for €190m, or just over 40% of the amounts raised. In 2024, ChapsVision and Zama represented €152m out of €352m, or more than 43% of the total. In 2025, concentration remained high, with Filigran and Zama together accounting for €99m out of €274m. In other words, despite the decline in the number of deals, the French ecosystem continues to produce several significant funding rounds each year.
Tikehau Capital's 2026 barometer confirms this resilience, while also showing a slight weakening of France's position in 2025. The barometer identifies 22 fundraising rounds in France, for a total of €221.6m in 2025, with an average ticket size of approximately €10.1m, compared with 25 fundraising rounds in 2024.

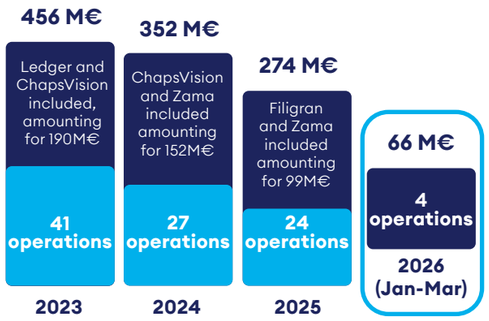
It also highlights that France remains a major player in Europe, ranking third in both amounts raised and number of deals in 2025.

This positioning should be understood in the context of a European market that has become more favourable again for cybersecurity.

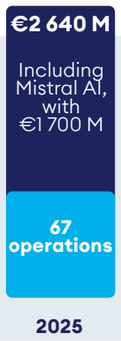
According to Tikehau, the number of cybersecurity fundraising rounds in Europe increased by 34% between 2024 and 2025, while the amounts raised rose by 83%, in contrast with the trend observed across all sectors. In other words, France is operating in a European market that has regained momentum, but where competition between national ecosystems has intensified, notably with the strong comeback of the United Kingdom and the solid performance of other markets.

Finally, 2025 also confirmed the ability of the French ecosystem to produce technology champions with global visibility. Tikehau's barometer notably cites Zama among the new global cybersecurity unicorns in 2025.

Amount of funds raised by French Digital Trust startups



Amount raised in AI in France



By comparison, fundraising in artificial intelligence reached much higher levels than those observed in cybersecurity in 2025. French AI companies raised €2.64bn across 67 deals, including €1.7bn for Mistral AI alone. Compared with the €274m raised in Digital Trust across 24 deals in the same year, these amounts place AI at a level nearly ten times higher in value and almost three times higher in number of deals. The Mistral AI transaction alone also accounted for nearly two thirds of the amounts raised in AI.
This difference does not call into question the strategic importance of cybersecurity, but illustrates the exceptional attractiveness of AI to investors, in a context where this segment concentrates a very significant share of growth expectations and technological transformation

List of fundraising activities of French Digital Trust startups

In 2024

	Company	Organisation	Year	Amount (M€)
1	ChapsVision	**ACN**	2024	85
2	Zama	**ACN**	2024	67
3	Filigran		2024	32.3
4	YesWeHack	**ACN**	2024	26
5	Stoïk	**ACN**	2024	25
6	Filigran		2024	15
7	Dfns		2024	15
8	BforAI		2024	14.4
9	Patrowl		2024	11
10	BforAI		2024	9.6
11	COMAND AI		2024	8.5
12	Tenacy		2024	6
13	Anozr Way	**ACN**	2024	6
14	Dotfile		2024	6
15	Probabl		2024	5.5
16	Mindflow		2024	5
17	Finovox		2024	3.9
18	Nijta		2024	2.1
19	Dipeo		2024	1.8
20	Alcyconie		2024	1.4
21	Kamae		2024	1.4
22	Nestor		2024	1.2
23	Daspren		2024	1
24	Soteria Lab		2024	0.8
25	Edamame		2024	0.4
26	Alphaguard		2024	0.2
27	LookUp Space		2024	
	Total ACN			**209**

In 2025

	Company	Organisation	Year	Amount (M€)
1	Filigran		2025	50
2	Zama	**ACN**	2025	49
3	Riot		2025	27.7
4	Sekoia	**ACN**	2025	26
5	Gatewatcher		2025	25
6	Dfns		2025	15.5
7	Qevlar AI		2025	13
8	Memority		2025	13
9	Evertrust		2025	10
10	BforAI		2025	9
11	Kerys		2025	6.2
12	CYGO		2025	5
13	Dastra		2025	4.3
14	Tremau		2025	3
15	Nucleon		2025	3
16	Plakar		2025	2.6
17	MokN		2025	2.6
18	Aleph		2025	2
19	Galink		2025	1.6
20	Skyld		2025	1.5
21	Akidaia		2025	1.3
22	Dream On Technology		2025	1.3
23	Avanoo		2025	1
24	Vaultys	**ACN**	2025	0.6
	Total ACN			**76**

In 2026

	Company	Organisation	Year	Amount (M€)
1	Riot		2026	25.5
2	Sekoia.io	**ACN**	2026	20
3	Cryptio		2026	15
4	CyGo Entrepreneurs		2026	5,4

POINT OF VIEW

Tikehau Capital - European Cybersecurity Investment Barometer

7th edition – March 2026

TIKEHAU CAPITAL

François Lavaste
Executive Director

As it does every year, Tikehau Capital, in partnership with the InCyber Forum, has published the **7th edition** of its cybersecurity barometer.

It has become a true benchmark and covers all financing and M&A transactions from **2025** in France, Europe, Israel, and the U.S

The first major trend of 2025 : Globally, cybersecurity funding continues to grow **with €15.6 billion raised across 866 transactions**, representing **a 29% increase in value and a 26% increase in the number of transactions**. The year 2025 thus set a **historic record** in terms of the number of funding rounds and ranked second only to the 2021 peak in terms of total funds raised.

In 2025, **Europe increases its share of the global market**, both in terms of funding raised rising from 9% in 2024 to 12% in 2025 and in terms of the number of deals, rising from 25% in 2024 to 26% in 2025.

In **Europe**, the cybersecurity sector clearly outperforms the tech sector as a whole :
while funding across all sectors is down slightly, **cybersecurity surges by 83% in funding raised**, **34% in volume**, with 226 deals–a **record**–driven by more mature funding rounds and primarily intra-European consolidation

In **France, cybersecurity investment activity remains at a high level with 22 funding rounds (vs. 25 in 2024) in terms of the number of deals**, but the amount raised drops to €221 million (vs. €342 million in 2024), as does the average deal size, which falls to €10.1 million (vs. €14 million in 2024). In 2025, for example, Tikehau Capital backed the company Memority with €13 million and announced a majority stake in Intersecc.

In conclusion, the overall assessment of 2025 is very positive, particularly at the global and European levels. It is becoming increasingly clear that the challenges in the cybersecurity and AI sectors are no longer just French but European. France, however, remains well-positioned, with the announcement of its first cybersecurity unicorn (Zama, a specialist in open-source cryptography). The year 2026 should confirm the establishment of **cybersecurity as a lasting pillar of innovation and European strategic independence**.

3.7 STRENGTHENING SMES AND TRENDS IN THE DEVELOPMENT OF THE START-UP ECOSYSTEM

1• The increasing maturity of Digital Trust SMEs

As shown in the infographic below, the French Digital Trust ecosystem has been built around large historical players, often originating from digital security and/or digital services, and frequently linked to sovereign and defence ecosystems. These large historical players, which are strong exporters, offer solutions aimed at governments, Operators of Vital Importance, and large international companies. They represent €17.6bn in revenue in 2025.

However, an ecosystem of SMEs specialised in Digital Trust began to emerge in the 1990s and is now consolidating its presence. During the 2010s, this ecosystem gradually gained in importance and now includes many large SMEs, some of which have already exceeded the €50m revenue threshold and become internationally oriented intermediate-sized enterprises. This ecosystem is composed mainly of cybersecurity start-ups, many of which offer solutions designed to address new markets, such as SMEs, micro-enterprises and small local authorities.

The strong growth of this ecosystem is driven by increasingly large fundraising rounds year after year. This ecosystem represents estimated revenue of between €2.8bn and €3.9bn in 2025, by aggregating SMEs with revenue above €5m, companies that have raised €5m or more, and SMEs that have become intermediate-sized enterprises since the 2000s.

Note: The companies whose logo is present in the box on the SME ecosystem correspond to the most remarkable: ISEs, companies that have benefited from the largest fundraising or SMEs with the largest revenue.

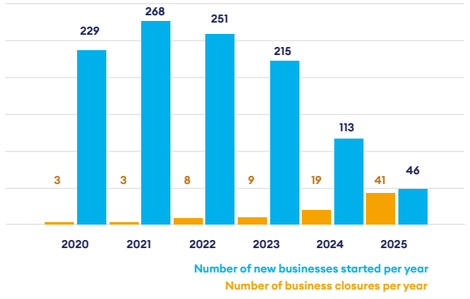
2• Recent developments in the start-up ecosystem: company creations, closures and insolvency proceedings

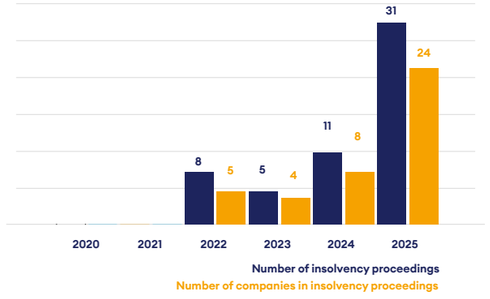
The start-up dynamic has followed a multi-stage trajectory. The years 2020 and 2021 were still shaped by the context of the health crisis and its effects on economic activity. The year 2022 marked the exit from the crisis, in a context where Digital Trust recorded, together with 2023, its strongest growth rates. This sequence resulted in a particularly high volume of company creations between 2020 and 2023, with 229 creations in 2020, 268 in 2021, 251 in 2022 and 215 in 2023. From 2024 onwards, the pace slowed, while remaining relatively sustained, with 113 creations, before declining more sharply in 2025, with 46 creations. In total, 1,129 companies were created over the observed period.

At the same time, company closures remained limited until 2023, with 3 closures in 2020, 3 in 2021, 8 in 2022 and 9 in 2023. The situation changed from 2024 onwards, with 19 closures, and worsened significantly in 2025, when 41 closures were recorded. In total, 98 companies closed over the observed period. This trend suggests that, after a phase of strong expansion in the entrepreneurial base, the ecosystem is entering a more selective phase, in which not all companies created during the high-growth years are able to stabilise their trajectory.

Insolvency proceedings confirm this development. No cases were observed in 2020 and 2021, before 8 insolvency proceedings were recorded in 2022, 5 in 2023, 11 in 2024 and 31 in 2025. In total, 66 insolvency proceedings were identified, involving 35 distinct companies. The gap between the total number of proceedings and the number of companies concerned shows that some start-ups experienced several successive events, indicating prolonged rather than one-off difficulties. The rapid increase in the number of companies concerned, from 5 in 2022 to 24 in 2025, highlights the spread of this phenomenon to a growing share of the entrepreneurial base.

Taken together, the indicators for company creations, closures and insolvency proceedings therefore point to a two-stage trajectory. The 2020–2023 period corresponds to a phase of strong entrepreneurial expansion, first in a crisis context and then in the post-crisis rebound and strong market momentum for Digital Trust. From 2024 onwards, and even more clearly in 2025, the ecosystem shifted towards a phase of rationalisation, marked by a slowdown in company creations and a visible increase in economic difficulties.





3• Forms of partnership within this ecosystem

Based on the survey and interviews conducted with industry players, French cyber start-ups appear to be part of an ecosystem in which relationships with established groups play an important role, but take various forms. According to the survey responses, partnerships with large companies are in place for some of the start-ups surveyed. These partnerships primarily take the form of commercial relationships and are generally perceived positively. Of the 7 usable responses, 3 start-ups reported having ongoing partnerships with large companies, mainly in the form of commercial contracts and, in one case, technological integration. Where they exist, these partnerships are considered useful, with an average score of 8.25/10 among the responses provided.

The interviews confirm that, in the French cyber market, established groups engage with start-ups according to several complementary approaches. The first is incubation and mentoring. This is the case for Thales. The group is STATION F's cybersecurity partner and has, for several years, structured a dedicated programme for cyber start-ups through the Cyber@Station F initiative, designed to support young companies working on Digital Trust and cybersecurity topics.

A second approach is technological co-innovation, in which the start-up provides a specialised building block while the established group brings industrialisation capabilities, customer access and credibility. This is illustrated by several cases mentioned during the interviews. At Thales, this approach is visible both in the cooperation showcased during European Cyber Week, where the group presented cyber demonstrators in connection with start-ups such as OverSOC, and in the strategic partnership announced in 2025 with Sekoia.io, aimed at integrating Sekoia's AI SOC platform into Thales' managed services, particularly in trusted environments such as S3NS. The interviews suggest that, beyond technological innovation alone, this type of cooperation also addresses the need to reduce the perceived risk for end customers, particularly in long-cycle sectors such as defence or nuclear, where the long-term viability of the supplier is a decisive criterion.

The interviews also underline that it is difficult for a French cyber start-up to be selected by large groups, which often tend to favour international suppliers that are already well referenced. In this context, the ability to showcase high-performing technology, an open architecture and a more competitive cost appears to be a key lever for differentiation. This reading is consistent with Sekoia.io's public positioning, which emphasises the openness of its platform, its many integrations and its anchoring in the French Tech 120, while promoting a European and sovereign approach to detection and response.

A third approach observed is the commercial and operational integration of start-up technologies into the offerings of already established cyber groups. Almond is an interesting case in this respect. On the one hand, Board of Cyber is publicly presented as a solution developed over three years within Almond's start-up studio. On the other hand, Almond has formed partnerships with several specialised start-ups, notably Memority on IAM issues and Qevlar AI for the integration of AI tools into its SOC. In the case of Qevlar AI, public communications highlight concrete operational gains, with the automation of a large share of alert processing and a significant reduction in remediation time.

The case of Sopra Steria highlights a corporate venture approach and the structuring of an innovation ecosystem. The group has a dedicated entity, Sopra Steria Ventures, which explicitly presents itself as an investment and strategic partnership vehicle for working with start-ups, with the aim of turning their technologies into concrete market offerings.

The survey also suggests that French cyber start-ups do not develop solely through the market, but also through their integration into research and public support schemes. Of the 7 responses collected, 4 start-ups reported participating in French or European cooperative R&D projects, mainly through France 2030 and, in one case, through a competitiveness cluster or labelled project. At the same time, access to public funding appears to be very widespread in the sample: all 7 respondents mentioned at least one scheme, in particular the Research Tax Credit, France 2030 and Bpifrance.

FOCUS

PUBLIC FUNDING FOR INNOVATIVE PROJECTS IN THE SECTOR - F. INITIATIVES

The Research Tax Credit (CIR), codified in Article 244 quater B of the General Tax Code (CGI), was established in 1983. It is a tax incentive mechanism designed to promote scientific and technical research efforts by companies. The CIR is a self-declaration system: unlike a grant, the audit process is random and takes place after the fact following the declaration. The tax authorities have three years to review the claim.

The CIR enables the financing of research and development ("R&D") and innovation activities by companies subject to corporate income tax.

Article 49 septies F of Annex III of the General Tax Code (CGI) defines a scientific or technical research activity that may be eligible for the CIR. Legal doctrine has clarified that the five criteria defined in the Frascati Manual must also be met.
Regardless of sector or size, all companies can benefit from the CIR.
In contrast, the Innovation Tax Credit (CII) is reserved for SMEs, as defined by the EU, that are not in financial difficulty. Note that the CII applies to prototypes or pilot installations of a new product, whereas the CIR applies to scientific or technical research activities.

As a "tax credit," if the CIR amount exceeds the tax liability, the taxpayer is entitled to a credit that may be refunded by the government. For example, if the taxpayer is an SME, they may receive an advance refund. Or, if this is not the case, they must first apply the CIR against their corporate income tax (IS) before, if applicable, requesting the remaining amount after a three-year period.

CIR rate*: 30% of eligible expenses (including subsidies) up to €100 million; 5% above that amount

CII* rate: 20% of eligible expenses, capped at €400,000 per year

*in Metropolitan France

Expenditure eligible for the CIR

- Personnel expenses
- Operating expenses
- Outsourced expenses – commonly referred to as subcontracting expenses
- Depreciation allowances
- Standardization expenses

Focus on the CIR reform – 2025 Finance Act

Since the 2025 Finance Act, patent fees, technology monitoring costs, and expenses for young PhDs have been eliminated. The operating expense threshold has been reduced from 43% to 40%.

Did you know?

In an amendment submitted during the 2026 Finance Act, MP Philippe Latombe proposed an amendment to create a digital CIR. With a preferential rate of 40% for sectors defined annually by decree, including AI, quantum computing, cybersecurity, blockchain, and digital biotechnology. This amendment was declared inadmissible and therefore could not be considered during a public session

At the same time, an amendment was introduced in the National Assembly and then in the Senate to extend CIR-eligible expenses to include costs related to renting computing time on GPUs and CPUs allocated to research operations by artificial intelligence companies.

To learn more about the CIR, download the F. Initiatives white paper "Research Tax Credit – 1983–2023: A Look Back at 40 Years of Funding" as well as its addendum on the implications of the 2025 Finance Act.

When it comes to grants:

- **You need to stay constantly** on the lookout for existing calls for proposals.
- **The funding agency** publishes its guidelines.
- **The project must not have started yet** in order to apply for funding.
- **You can choose to submit your project on your own, or as part of a collaborative project** – meaning you will sign a consortium agreement, outline the division of tasks, establish how intellectual property rights for project outcomes will be shared, and define the process for publishing and disseminating results, etc. by appointing a coordinator responsible for managing the project on behalf of the funder.

The "Pioneers of Artificial Intelligence" call or proposals aims to support R&D projects with high potential for economic impact that contribute to national sovereignty through disruptive innovations in artificial intelligence.

Its funding has been divided into three phases:
- **a phase to fund the technical feasibility of the proposed solution**, which is based on disruptive technology
- **a phase for more ambitious** developments
- and finally, **a final phase to fund the application of the work carried** out on an economically promising use case and the realization of a prospect for the industrialization and commercialization of the developed solution.

POINT OF VIEW

ABBAS DJOBO'S POINT OF VIEW

F. INITIATIVES

Abbas Djobo
F.initiatives President

As president of F. Initiatives, a company specializing in innovation financing, what advice do you have for companies filing for CIR?

"First and foremost, keep in mind that we are talking about public funds: an investment by the government and therefore by each and every one of us aimed at encouraging R&D and innovation activities and thereby boosting our country's competitiveness. Public funds imply the possibility, if not the necessity, of oversight.
Be sure to anticipate this oversight and rigorously collect supporting documentation both before and as research activities are carried out; ensure these activities are properly structured before they begin and throughout the process; pay particular attention to tracking researchers' time."

A unique aspect of our sector is that we do not have an APEC or NAF code to identify us. Who is eligible for public funding?

"This is where the full power of the Research Tax Credit lies: we are talking about indirect support aimed at fostering R&D and innovation activities. To achieve this goal, policymakers have recognized that research is present in all sectors of activity and can be conducted by any type of company.
This public support is likely to be of greater and more practical importance in sectors where research activities are less obvious or less developed; thus, the CIR applies to all sectors, from SMEs and startups to large corporations; only the research project itself, its eligibility, and the supporting documentation matter.
I cannot emphasize enough the importance of documentation: being able at all times to substantiate the reality of one's work."

What documentation is required to file a CIR declaration?

"In addition to the reporting requirements (Cerfa 2069), it is important to compile all relevant documents into a supporting file: a detailed description–without being overly extensive is necessary; the objective here is to describe the work, demonstrate its eligibility (work carried out beyond the state of the art), and include any elements that establish its reality and significance. Even though it is not mandatory, I recommend using or drawing inspiration from the template provided by the Ministry of Research in its annual guide."

"Declaring a CIR project cannot be improvised. Substance is the cornerstone of a well-founded declaration."

Does your company also use artificial intelligence to deliver its services?

"As you know, AI will never replace humans, nor will it carry out research work on your behalf... at least not within the scope of the CIR. AI is a remarkably effective tool to help you structure and formalize your work. F.initiatives has been quite visionary on this subject by creating its own internal research laboratory several years ago: our researchers, authors of international publications, have thus been able to create several tools to assist our consultants and clients. Neophi, a superb tool for conducting scientific literature reviews, is a perfect example. All of these developments are governed by our ISO 42001 certification to ensure transparency, security, and, of course, strict ethical standards."

Finally, a closing remark?

"Filing a CIR declaration cannot be improvised. Materiality is the cornerstone of a well-founded declaration. I would add that the CIR should not be an end in itself or a goal; what matters above all is your research strategy, your project, and the impact you can have on your company and your industry. The CIR will support you in this endeavor."

NeoPhi

Discover NEOPHI, designed by researchers, for researchers!

https://www.neophi.ai/fr

3. KEY FIGURES OF THE INDUSTRY
ACN Observatory of Digital Trust Sector 2026

4. TRUSTED AI: CHALLENGES AND PROSPECTS FOR THE FUTURE

4.1 The artificial intelligence value chain

4.2 Generative or specific artificial intelligence: different data requirements

4.3 Specific AI generates more value than general-purpose AI in France

4.4 The rise of agent-based AI in cybersecurity

- Point of view: Alignment, the key to trust in AI systems
  Vanina Paoli-Gagin – Senator for Aube

4.1 THE ARTIFICIAL INTELLIGENCE VALUE CHAIN

Trustworthy Artificial Intelligence emerged in 2024 as a new segment of the French Digital Trust sector, alongside digital security and cybersecurity products and services.
This chapter positions the French sector along the trustworthy artificial intelligence value chain (1), and distinguishes between generative AI and specific AI in terms of data requirements and value creation for the French sector (2). Finally, this chapter examines the rise of agentic AI applied to cybersecurity, which represents one of the most notable recent developments in the trustworthy AI sector.

The Artificial Intelligence Value Chain

Processor manufacturers: a structural dependence on US players

The production of artificial intelligence depends, upstream, on manufacturers of specialised processors – GPUs, NPUs, ASICs, etc. – required for model training and inference. This segment is dominated by US companies such as NVIDIA, AMD and Intel. These companies, often fabless, focus on the electronic design of chips, which are then manufactured by foundries, mainly in Asia, particularly by TSMC in Taiwan. Hyperscalers such as Google and AWS are also investing in this segment by developing their own chips, such as TPUs and Trainium.
France is almost absent from this critical stage. A few rare fabless companies, such as SiPearl, VSORA and Kalray, are seeking to position themselves, but the ecosystem remains modest and nascent. Major European semiconductor producers, such as STMicroelectronics, NXP and Infineon, focus on embedded markets – automotive, aerospace, defence, etc. – and do not aim to invest in competing with US giants in artificial intelligence chips.

Datacentre equipment manufacturers, supercomputers, etc.: a limited French presence

The hardware equipment segment – high-performance computing servers and supercomputers – is dominated by US and Chinese players such as HP, Dell, IBM and Lenovo. These players source processors from manufacturers in order to assemble infrastructure solutions tailored to the needs of artificial intelligence. The two French players with a significant role in this segment are Atos – through its Bull subsidiary – and, to a lesser extent, OVH. These two companies design the architecture of their servers and assemble them. However, this French presence remains isolated and fragile in a sector characterised by intense international competition. French capabilities are far from matching those of the major US and Chinese industrial players.

Cloud service providers: a market dominated by hyperscalers

Cloud service providers offer the infrastructure required to train and deploy artificial intelligence models. Global leaders – AWS, Microsoft Azure and Google Cloud – have massive computing capacities and also offer their own AI technology building blocks, such as GPT, Vertex AI and Azure OpenAI, thereby becoming both hosting providers and software publishers. France is seeking to build an alternative ecosystem, with players such as OVHcloud, Numspot, Outscale, Docaposte, Platform.sh and Scaleway. Alongside these infrastructure offerings, some French players are also developing platforms designed to industrialise AI use cases in sovereign environments. This is the case for Sopra Steria with Innerdata, presented as a machine learning operations platform and a data/AI platform intended to support the scaling-up of artificial intelligence strategies, including in trusted environments.

Generative AI

Artificial intelligence software publishers: a rapidly growing French dynamic

Software publishers develop software solutions based on artificial intelligence, most often commercialised as application services, or SaaS. This segment covers two broad categories of players:
• Publishers of generic models, which design foundation models – LLMs, diffusion models, etc. – intended to be used or adapted in various contexts.
• Publishers of business-specific solutions, which develop tailor-made models to address specific needs in a given sector.
In France, Mistral AI – which develops open-source, general-purpose LLMs – is one of the few players in the first category. In the second category, there are many French companies designing their own models adapted to targeted data and specific problems:
Shift Technology for insurance fraud, Gleamer for radiology, Exotec for logistics robotics, Dental Monitoring for orthodontic monitoring, and Wintics for video analytics for cities and infrastructure. These solutions sometimes rely on the adaptation of external models, but are always designed as standalone products.
Internationally, a similar structure can be observed: publishers of generalist models, such as OpenAI, Anthropic and Cohere, and specialised publishers, such as Tempus in healthcare, Darktrace in cybersecurity, Trax in retail intelligence, and SambaNova in scientific and industrial analytics.

Specific IA

Digital services companies

Digital services companies play a key role in the practical deployment of artificial intelligence within businesses. They develop tailor-made models based on their clients' data, information systems and business objectives.

They also provide integration, consulting and support for the implementation of artificial intelligence. France benefits from a very strong network of companies such as Sopra Steria, Capgemini, Atos, Thales, Orange Business and Wavestone.

Integrators

Integrators provide the link between technologies – models, software, APIs, etc. – and concrete business use cases, particularly in industrial or sovereign sectors. They deploy solutions in specific business environments, often combining them with other technological building blocks or embedded systems. These players play a structuring role in the diffusion of artificial intelligence within the economy by integrating it directly into complex systems or equipment. Thales, Airbus Defence & Space, Idemia and Safran are among the major integrators in the Digital Trust sector. France also has major integrators in other sectors, such as energy, automotive and healthcare.

Note: this visual positions the most emblematic French and foreign players in each segment. Consequently, the absence of a company's logo from a given segment does not mean that the company is absent from that segment. For example, Thales is positioned both in the AI software publishing segment, in the digital services segment and in integration.
Source: DECISION Etudes & Conseil

4. TRUSTED AI: CHALLENGES AND PROSPECTS FOR THE FUTURE
ACN Observatory of Digital Trust Sector 2026

4.2 GENERATIVE OR SPECIFIC ARTIFICIAL INTELLIGENCE: DIFFERENT DATA REQUIREMENTS

Generative artificial intelligence refers to models capable of producing new content – text, images, sound or video – from textual, visual or voice instructions. These models, such as LLMs, or Large Language Models, and SLMs, or Small Language Models, are pre-trained on vast volumes of generalist data. They can then be adapted to various uses: text generation, information classification, planning, product or service recommendation, or chatbots and virtual assistants.

The French sector has several players positioned in this segment:

• **Mistral AI** is the emblematic French start-up in the sector, specialising in the development of open-source, general-purpose LLM models used for generation and dialogue tasks.

• **DALVIA Santé** is Docaposte's medical assistant based on generative AI, enabling the production of hospital discharge reports from audio notes and documents from the patient journey. Hosted on the sovereign cloud NumSpot, the solution is designed to guarantee data security and integrate with hospital business software. It aims to save time for healthcare professionals while improving coordination between stakeholders.

• **Assist'Act** is Docaposte's tool to support the drafting of administrative acts for local authorities, incorporating a conversational assistant based on artificial intelligence. It enables the generation, search and optimised management of public acts.

• **IRIS**, developed by Sopra Steria in partnership with IBM and IVèS, is the first conversational assistant in sign language. This "signbot" enables real-time interactions in French Sign Language, Quebec Sign Language, American Sign Language and Tunisian Sign Language, combining conversational AI via IBM Watson with the accessibility solutions developed by IVèS..

Specific artificial intelligence, by contrast, refers to solutions designed for precise use cases in defined business environments. These AI systems rely on highly targeted input data – text, sound, images, video, signals, time series, etc. – and are trained on more limited but highly qualified volumes of data. They can be used, for example, to automate document reading, detect visual anomalies, predict failures or detect risky behaviours.

The French sector has a large number of players that are very well positioned in this segment:

• **Safran AI** develops algorithms for the automatic analysis of high-resolution satellite images, Full Motion Video and acoustic signals. These solutions, intended for the defence sector, enable the detection of objects or events of military interest. They are based on a secure processing chain with full data traceability and are designed to be integrated into critical systems.

• **Gleamer** offers a solution for analysing bone lesions from medical images and generates an automated preliminary diagnosis for radiologists. The practitioner remains responsible for validating the report. The solution is deployed in more than 50 hospitals and clinics in France, including Hôtel-Dieu and Ambroise Paré, and was awarded the Best New Radiology Vendor Award at the Eurominnies 2023.

• **Wintics** offers an intelligent video analytics solution to improve infrastructure security, traffic flow and urban planning. These tools enable local stakeholders – airports, ports, public transport operators, local authorities, etc. – to make decisions based on the analysis of behaviours, flows or anomalies detected in public spaces.

Data requirements vary depending on whether the AI in question is generative or specific. Generative AI relies on access to enormous volumes of heterogeneous data, often taken from the web or from large textual corpora. The aim is to maximise the coverage and diversity of the data in order to enable models to learn how to generate relevant content across a wide range of contexts. This Big Data logic raises major ethical issues regarding access to large datasets in order to remain competitive with US or Chinese solutions, particularly in sensitive sectors such as healthcare, education and transport.

By contrast, specific AI relies on targeted, business-specific and highly qualified data. These models are designed for restricted use cases and require more modest but perfectly structured, annotated and contextualised datasets.

The emphasis is placed far more on data quality than on data quantity. In this context, training can often be carried out locally, without massive computing infrastructure. One example is Safran AI, whose teams include specialised analysts responsible for manually annotating the satellite images used to train the algorithms.

This human annotation guarantees maximum precision, enabling models to finely distinguish objects or anomalies of interest. This iterative approach, based on data quality and business expertise, limits the need for massive infrastructure while ensuring high levels of performance in critical contexts such as defence and security.

4.3 SPECIFIC AI GENERATES MORE VALUE THAN GENERAL-PURPOSE AI IN FRANCE

Within the framework of this Observatory, the analysis of artificial intelligence production in France focuses on "trustworthy" artificial intelligence, meaning artificial intelligence designed and deployed in accordance with a set of legal, technical and ethical criteria. This concept combines the principles set out in the White Paper of the Alliance pour la Confiance Numérique — transparency, explainability, robustness, security, privacy protection and human oversight — with a sovereignty dimension, explicitly incorporating the criterion of company nationality. Solutions designed by French players are therefore considered to form part of this trustworthy production.

Despite the media and financial enthusiasm generated by generative AI – particularly since the emergence of LLMs such as GPT and Claude, or open-source models such as those developed by Mistral AI – specific AI accounted for 78% of the revenue generated from France in 2025, or €1.5 billion, compared with only 22% for generative AI, or €437 million.

This gap between visibility and economic reality continues to be reflected in fundraising.

In 2025, generative AI and generalist models once again attracted the most visible funding rounds, in particular Mistral AI with €1.7 billion, but also players positioned on application building blocks for content generation or processing, such as Moments Lab with €24 million, Aive with €12 million, Arcads AI with €14 million and PyannoteAI with €8.1 million. At the same time, companies associated with more specific AI, integrated into precise business use cases, confirmed their dynamism through a growing number of mid-sized funding rounds across a variety of sectors.

This was notably the case for BforeAI, with €9 million, and Qevlar AI, with €13 million, in cybersecurity; DeepIP, with €15 million, in intellectual property; Veesion, with €38 million, in computer vision applied to retail; and Nabla, with €65 million, and SeqOne, with €20 million, in healthcare. Thus, beyond a few highly publicised mega-rounds, 2025 above all confirmed the broadening of the French AI market to include a set of specialised players positioned on increasingly diverse sector-specific use cases and business functions.

More broadly, the trustworthy AI segment remained relatively immature in 2025, with average revenue per employee far lower than in other Digital Trust segments, at €84,000.

4.4 THE RISE OF AGENT-BASED AI IN CYBERSECURITY

One of the most significant recent trends within the trustworthy AI sector is the rise of agentic AI applied to cybersecurity. Agentic AI is understood here as systems capable of linking together, under human supervision, several stages of analysis, investigation, decision-making and execution within a single operational process. This evolution marks an important shift: AI is no longer used only to assist an analyst on a one-off basis or to generate content, but to automate end-to-end certain critical tasks relating to incident detection, qualification and response.

This dynamic is already taking shape among several players in the sector. In February 2026, Sopra Steria introduced agentic workflow functions into its IAKA platform in order to orchestrate AI agents capable of linking several stages of analysis and production within complex processes, while remaining integrated into existing business systems and under operator control. Sekoia.io, for its part, positions its AI-SOC platform around the automation of detection and response, and explicitly stated in 2025 that it intended to accelerate its investments in agent-based AI; the company also emphasises that a significant share of the threats detected by its platform have already been detected automatically through its AI and cyber threat intelligence technologies.

Almond also illustrates this evolution through its partnership with Qevlar AI, which aims to industrialise the automated investigation of cyber incidents within the SOC and to significantly reduce remediation times for a large proportion of the alerts processed.

The rise of agentic AI in cybersecurity concerns not only major integrators and digital services companies, but also specialised software publishers. In 2025, WALLIX strengthened its AI strategy through the acquisition of the French start-up Malizen, which specialises in the analysis of cybersecurity data using artificial intelligence.

At European level, the €10 million fundraising round completed by Equixly in December 2025 also confirms investor interest in agentic AI solutions applied to offensive security and automated API security testing.

Value creation is no longer located solely in hosting infrastructure or generalist models, but increasingly in software building blocks capable of automating complex cyber operations using sensitive and contextualised data.

From this perspective, agentic AI appears to be a natural extension of trustworthy specific AI. It relies less on access to the largest volumes of generalist data than on the ability to mobilise business data, expertise, operational scenarios and secure environments. For the French sector, the strategic challenge is therefore less about competing head-on with hyperscalers across the entire generative AI value chain than about structuring vertical, sovereign and integrated offerings capable of combining cyber expertise, advanced automation, human supervision and high trust requirements.

POINT OF VIEW

ALIGNMENT: A PILLAR OF TRUST IN AI SYSTEMS

Vanina Paoli-Gagin
Aube department Senator
(Grand Est region)

“ Alignment is not just about avoiding a crash; it is also about addressing an issue that combines sovereignty, competitiveness and our model of society, or even of humanity. ”

Every technological revolution brings with it its share of fears, fantasies, and resistance. When the first airplanes appeared, some claimed that the human body could never withstand such speeds. These predictions, however, remind us of a constant: when faced with innovation, legitimate concerns always coexist with vested interests, information asymmetries, and protective reflexes.

Artificial intelligence (AI) is no exception. It inspires immense hope, but also deep concern, which is not irrational.

AI is already transforming our relationship to work, knowledge, information, decision-making, and creation. It is reshaping the balance of political and economic power, blurring the lines between assistance, automation, and delegation, and erasing the boundaries between dream and reality. It creates new opportunities, but also new vulnerabilities, as it profoundly transforms humanity’s relationship with the world.

The wrong answer would be to choose between two equally unproductive stances: outright rejection or blind acceptance.

No doubt the right question lies elsewhere: under what conditions can we, and are we willing to trust AI? This trust, a rare commodity of our century, is built neither through marketing, nor through incantation, nor through the mere promise of future economic progress. It rests on an existential requirement: the alignment of AI systems.

An AI system is aligned when its actual behavior remains consistent with human intentions, the limits set for it, and the values we deem legitimate. This very concrete definition raises a simple question: how can we ensure that a system, capable of becoming autonomous, ever more powerful and widespread, continues to do what we actually expect of it?

A system is not trustworthy simply because it functions in a demonstration or experimental setting. It is trustworthy only if we can verify that it remains reliable, controllable, and robust under real-world conditions, in open and sensitive environments, under stress, and in the face of the unexpected.

This requires making systems understandable, controllable, and governable through evaluation methods, verification capabilities, standards, audit mechanisms, and chains of accountability.

This challenge becomes critical as AI becomes established in sectors where failure is unacceptable: defense, critical infrastructure, healthcare, finance, education, and public services.
To continue the aviation metaphor, the goal is not to arbitrarily limit the plane’s speed, but to ensure that the pilot maintains a reliable aircraft and control over its trajectory to bring passengers safely to their destination.

It is, I believe, in this spirit that the Prime Minister entrusted me, in late February, with a parliamentary mission on the alignment of AI systems. The objective is clear: to map out the relevant stakeholders, inventory existing initiatives, assess the technical, economic, institutional, and ethical conditions for effective alignment, and identify the levers that will enable France and Europe to position themselves on this strategic issue.

For alignment is not just about avoiding a crash; it also involves a challenge that combines sovereignty, competitiveness, and our model of society and even of humanity.

For AI to be adopted widely, usefully, and sustainably, we must be able to demonstrate that it remains compatible with our democratic principles, our security requirements, and our conception of responsibility, including environmental responsibility.

If we want to influence the development of international standards that drive markets, let us adopt a proactive stance by making alignment a field of excellence and a lever for competitiveness for France and Europe.

As this mission progresses, I am deeply convinced that we must build a genuine industrial ecosystem for alignment, bringing together researchers, industry leaders, public stakeholders, evaluators, and standard-setters, all the way to end users.

AI will not wait for us to finish debating it. The question is therefore simple: do we merely want to go along with the trend, ultimately being at its mercy, or do we want to be its driving force by defining its objectives and establishing the rules and safeguards we desire?

Tomorrow’s digital trust will not be won against AI, but through our ability, in a context where the line between reality and fiction will grow increasingly blurred, to make it an aligned technology.

5. CURRENT STATUS OF ONLINE THREATS

5.1 ANSSI Cyber Threat Overview 2025
5.2 Insights from industry experts
• Focus: DOCAPOSTE-CYBLEX Cybersecurity Barometer 2025

5.1 ANSSI'S CYBERTHREAT OVERVIEW 2025

The 2025 Cyberthreat Overview published by ANSSI provides a thorough assessment of a cyberthreat landscape that remains high, diverse, and systemic in France and Europe

ANSSI 2025 Cyber Threat Overview

available at the following link:
urlr.me/SDbxBj

The year 2025 is characterized by increasingly complex attacks, a growing blurring of the lines between state actors and cybercriminals, and more sophisticated offensive techniques. ANSSI handled 3,586 security incidents in 2025, representing an 18% decrease compared to 2024, partly attributable to the exceptional spike in reports linked to the Paris Olympics. Despite this decline, the number of confirmed incidents remained stable at 1,366, with a marked concentration in four sectors : education and research (34%), government ministries and local authorities (24%), healthcare (10%), and telecommunications (9%).

In terms of motives, attacks for financial gain, particularly via ransomware, remain dominant, with 128 incidents recorded in 2025, compared to 141 in 2024. SMEs, micro-enterprises, and mid-sized companies remain the primary targets, but healthcare facilities saw their share rise to 8%, while primary and secondary schools were particularly affected. A concerning trend is the adoption of ransomware by state-sponsored actors, notably North Korean and Chinese ones, further blurring the line between cybercrime and espionage. At the same time, unencrypted data exfiltrations are increasing significantly, with 196 incidents recorded in 2025 compared to 130 in 2024, often attributed to groups exploiting zero-day vulnerabilities, such as the one affecting Oracle E-Business Suite.
The use of infostealers as a vector for initial intrusion is also intensifying.
Strategic espionage conducted by state-sponsored actors, particularly Russian and Chinese ones, remains a major threat. Modus operandi (MOA) such as Laundry Bear (Russia), RedDelta/Mustang Panda (China), and Salt Typhoon primarily target diplomatic and government entities, critical infrastructure, and the defense sectors.
These actors exploit software vulnerabilities and advanced social engineering techniques, such as SIM swapping or MFA Fatigue, to gain access to sensitive information. At the same time, destabilization operations, including denial-of-service (DDoS) attacks and attempts to sabotage critical infrastructure, are on the rise. In France, pro-Russian hacktivists are targeting small industrial facilities exposed on the internet, although the physical impacts remain limited.

Innovation in offensive capabilities is a key trend in 2025. Attackers are massively hijacking legitimate tools, such as cloud services (Google Drive) or development platforms (Pipedream), to evade detection and reduce their operational costs.

Generative artificial intelligence is also being exploited to automate personalized phishing campaigns or to corrupt model training data.

Social engineering techniques are diversifying, with campaigns encouraging victims to execute malicious commands themselves, or voice attacks impersonating trusted authorities. ANSSI notes increased collaboration among malicious actors, whether through tool sharing, the reuse of exploited vulnerabilities, or the outsourcing of attack phases via initial access brokers. This interpenetration between criminal and state ecosystems complicates the attribution of attacks, especially as internal data leaks reveal personal ties between cybercriminals and intelligence services, without necessarily proving systematic coordination.

However, technical vulnerabilities remain the most exploited intrusion vector, with recurring targeting of edge devices–such as firewalls, VPNs, and SharePoint solutions–as well as zero-day exploits. Incidents handled by ANSSI highlight persistent gaps in patch management : in 2025, more than 6,200 French assets were still vulnerable to critical vulnerabilities disclosed since 2023. Supply chain attacks are becoming widespread, affecting both industrial subcontractors within the Defense Industrial and Technological Base (BITD) and cloud service providers, whose compromise can impact hundreds of customers. The education sector, which is often poorly secured, and mobile environments, through the exploitation of iOS/Android vulnerabilities, are frequent entry points.

In light of this, ANSSI emphasizes the importance of collective resilience, reinforced by the implementation of the NIS2 Directive and the Cyber Resilience Act, which will very soon impose heightened security obligations on critical operators. The complexity of digital environments and the volatility of threats–with the average lifespan of a ransomware group estimated at 262 days–require constant monitoring and continuous adaptation of defenses. ANSSI's recommendations–such as conducting comprehensive audits of information systems, separating professional and personal use, and securing VPN access–highlight a key imperative : cybersecurity must now be approached as a strategic issue that integrates human, legal, and geopolitical dimensions.

34 %
of cyber incidents in 2025 affected the education and research sector.

48 %
of ransomware attack victims are small and medium-sized enterprises (SMEs), micro-enterprises, and mid-sized companies, representing an 11% increase.

18 %
annual increase in the number of vulnerabilities disclosed since 2020.

5.2 INSIGHTS FROM INDUSTRY EXPERTS

RED ALERT LABS

Roland ATOUI
CEO

CRA 2026: from regulatory requirement to operational challenges

“By 2026, the cyber threat will no longer be merely technical: it will also be regulatory. With the implementation of the Cyber Resilience Act, companies will have to demonstrate the cybersecurity of their products throughout their entire lifecycle, from design to vulnerability management. The main challenge will not be understanding the text, but translating it into concrete evidence, processes, and decisions–often within complex supply chains. Those who prepare early will turn this constraint into an advantage. This is precisely where structured support and platforms like CyberPass come into their own.”

YesWeHack

Aïmad BERADY
Chief Product Officer

Hide those “vulnerabilities” from me - I wouldn’t know how to handle them!

“The cybersecurity industry is undergoing an alarming shift: the accumulation of security events labeled as “vulnerabilities” is overwhelming backlogs. Buried under alerts from automated scanners lacking context, teams are exhausting themselves on pseudo-incidents at the expense of truly impactful vulnerabilities. This race for exhaustiveness creates a false sense of security. To regain true resilience, it is necessary to separate the noise from the signal while keeping the human element at the heart of the system. The cybersecurity expert, augmented by AI as needed, remains the only one capable of understanding the business context, proving exploitability, and assessing the actual risk. The challenge is no longer to blindly patch issues, but to collect, focus on, and neutralize only what threatens the organization”

THALES
Building a future we can all trust

Christophe BIANCO
VP Cybersecurity Services

By 2026, cybersecurity will be a prerequisite for trust on a global scale.

“The rise of AI intensifies threats: automated attacks, targeted phishing, and targeted AI models. Organizations are responding with AI-enhanced cybersecurity, more resilient or even semi-autonomous SOCs, and integrated IT/OT monitoring. Hybrid campaigns involving both nation-states and cybercriminals are on the rise, while protecting supply chains and OT environments remains critical. Quantum risk and “Harvest Now, Decrypt Later” tactics demand agile cybersecurity, supported by NIS2, DORA, and the Cyber Resilience Act. 2026 is a pivotal year: cybersecurity is no longer merely a shield but a competitive advantage and a prerequisite for global trust.”

v6Protect

Florian BOMBARD
President

AI: the new fuel for cyber threats

“AI has opened new doors for attackers: no coding is needed; simply training a model is enough to design and launch an attack. Attacks are becoming more stealthy, precise, and impactful, rendering conventional defenses ineffective. Two trends are emerging in 2025/2026. First, bots are evolving and adapting: AI bot traffic has surged by 300% since July 2024, while DDoS attacks have increased by 94%. Second, cybercriminals are targeting APIs and LLMs on a massive scale, as these have become the new goldmine for monetizing critical data. Faced with this growing threat, companies must map and reduce their attack surface and rely on behavioral analysis to protect their digital services.”

iDAKTO

Yann BOUAN
Chief Strategy Officer

Identity governance: a systemic challenge for cybersecurity

“Behind the most significant incidents of 2025 lies the same mechanism; the attacker did not force entry: insufficient authentication, poorly defined service provider boundaries, and excessive storage of personal data; these are all structural vulnerabilities that precede any technical failure. An organization’s attack surface is measured by the total number of identities it manages–or fails to manage. Reducing collected data to the bare minimum and controlling every access point in the chain are the two most fundamental security decisions.”

Phragma.

Frédéric CERCLET
Manager

Digital Identity: better protecting our data

“Data breaches have become a daily occurrence, affecting all sectors of activity. The reality is alarming: every French citizen’s data is reportedly stored in at least one compromised and resold database. Despite the GDPR, the protection of data entrusted to third parties remains a failure. The consequences are very real: identity theft and targeted phishing are on the rise, compounded by deepfakes that make scams increasingly difficult to detect. The digital identity wallet envisioned by eIDAS v2 aims to reduce these leaks: each citizen will share only the information strictly necessary. A promising step forward, provided it is accompanied by awareness-raising and a robust public-private ecosystem. A significant challenge for industry players and digital audit providers!”

iliadata

Julia CHAULET
CEO & Co-founder

Rethinking digital trust in the era of systemic threats

“Massive data breaches and current geopolitical tensions reveal a reality: trust in digital infrastructure is no longer a given. In this context, traditional security models are reaching their limits, even as organizations must balance data protection with technological autonomy. It has become necessary to fundamentally rethink who controls, processes, and protects data, while acknowledging an inescapable reality: the loss of control over infrastructure. In this framework, cryptography emerges as a strategic lever, providing robust technical guarantees.”

sekoia

François DERUTY
Chief Intelligence Officer

The CTI: a strategic compass in a fragmented cyberspace

“ In 2025–2026, geopolitical instability reshapes the threat. We are witnessing an unprecedented hybridization: state-sponsored sabotage or espionage operations draw inspiration from cybercriminal tactics, and vice versa. Faced with adversaries who pool their infrastructure, purely reactive defense is blind. This is where Cyber Threat Intelligence (CTI) becomes vital. It is no longer a luxury, but the engine of anticipation. By deciphering modus operandi and contextualizing the threat, CTI enables organizations to dynamically adapt their posture. In the face of the current geopolitical fog, natively integrating intelligence into the core of security operations is the only way to transform uncertainty into true cyber resilience. ”

citalid

Alexandre DIEULANGARD
Co-founder and CEO

Neither panic nor denial : AI requires a nuanced assessment of risk

“ In 2025 and 2026, artificial intelligence (AI) has proven to be an operational multiplier for threat actors: more credible social engineering, better-contextualized fraud, and more subtle detection indicators. The impact is real, but gradual–a far cry from the disruptive scenarios that dominate public discourse. Yet it is precisely this gap between reality and perception that constitutes the most concrete decision-making risk. Discourse oscillates between overestimating offensive capabilities and excessive confidence in existing safeguards–two biases that lead to inappropriate trade-offs. The most resilient organizations are those that maintain a factual and proportionate perspective: AI amplifies known attacks; it does not reinvent them. ”

BYCYB
build your cyber

Sébastien FAUX
CEO

Cybersecurity and AI: why organizations are struggling to keep up, according to ANSSI

“ ANSSI’s 2025 Cyber Threat Landscape is clear: the threat remains high, affects all stakeholders, and blurs the lines between cybercrime and state-sponsored actions. But what is changing profoundly is the role of AI. Attackers are now exploiting generative AI to create more credible phishing attempts, produce malicious scripts, or clone voices during vishing attacks. The result: even less-skilled attackers can now carry out more sophisticated operations. In this context, simply claiming to be “secure” is no longer enough. In the face of stricter regulatory requirements, notably NIS2 and the CRA, independent assessment allows for an objective evaluation of the measures actually in place, identifies blind spots, and provides concrete evidence of compliance. ”

NANO CORP.

Franch FRANCIS
CEO

What you don’t see is already putting you at risk

“ In 2026, the cyber threat is no longer distinguished by its sophistication but by its ability to exploit blind spots. Indeed, a growing portion of infrastructure remains invisible: non-agent-managed systems, hybrid environments, etc. As long as security relies on a partial and declarative view, it will remain circumventable. Two priorities for 2026: Achieving comprehensive, real-time visibility into communications between systems–including where no agents or reliable logs exist–is a priority. Continuously mapping assets (dependencies and behaviors) to detect exploitable gaps. Without this factual foundation, every new tool adds noise, not control. ”

ORYOL
CYBER SOLUTIONS

Ramzi KHECHAIMIA
CEO and Co-founder

Cybersecurity 2026: the era of operational sovereignty

“ By 2026, the cyberthreat is automated, coordinated, and systemic. AI now enables attackers to exploit organizational vulnerabilities in real time, infiltrating their supply chains and partners. Every link in the chain has become critical. NIS2, DORA, and CRA impose unprecedented requirements without dictating how to meet them. Against this backdrop, the issue of operational sovereignty has emerged as a concrete priority. The sovereign SOC is establishing itself as a foundational solution: maintaining control over detection, reducing response times, and preserving decision-making autonomy. Automation plays a central role, but human expertise remains decisive in the most sensitive decisions. ”

sopra steria

Fabien LECOQ
CEO Business Line Cyber Group

Cybersecurity : strength through serenity

“ The year 2025 confirmed an escalation of the cyber threat targeting European organizations. In 2026, this threat has become a permanent fixture at the heart of digital value chains and critical ecosystems. State-sponsored actors are prioritizing strategies to establish a foothold in critical infrastructure, while cybercrime continues to become increasingly industrialized. AI amplifies these dynamics by automating attacks and enhancing social engineering on a large scale. In this context, the line between espionage, influence operations, and cybercrime is blurring. For European organizations, the challenge will be less about preventing all intrusions and more about detecting, understanding, and containing adversarial operations in order to sustain digital trust over the long term. ”

Loria

Philippe LOUDENOT
DPO Director of Cybersecurity Strategy

Cyber Threats 2025–2026: silent and pernicious leaks

“ The objective of the M32 autonomous agent is to infiltrate a high-tech company; it embeds the latest updates and can be considered one of the most advanced Autonomous Cyber Weapon Systems (ACWS). M32 studied its target and launched the attack. After several weeks of infiltration, the M32 agent exfiltrates relevant information and corrupts sensitive data. AI’s capacity for analysis, generation and decision-making makes it possible to envisage the construction of SACA, like the fictional M32 agent. cyberattack campaigns could then be fully automated, amplifying the number of attacks, their speed of execution, and amplifying the consequences and damage. ”

ANOZR WAY

Philippe LUC
Co-founder

Human risk management at the heart of cybersecurity in 2026

“ By 2025, social engineering has reached a new scale, driven by AI automation and the massive exploitation of stolen data: ANOZR WAY has identified over 2.6 billion compromised data records. At the same time, studies agree: generic training and phishing campaigns are no longer sufficient to reduce human risk. 2026 marks the beginning of a phase of industrialization in human cyber risk management. Human risk is no longer a matter of awareness but is integrated into the core of business operations–identity management, detection of behavioral vulnerabilities, and personal insurance. For ANOZR WAY, this is already translating into a sharp increase in requests for interoperability and partnerships to address new large-scale use cases. ”

Patricia MOUY
Head of the Cybersecurity Program at CEA-List

Anticipating threats through research

“ Faced with the continued rise of digital technology, the expansion of the attack surface, and the growing complexity of threats, a purely reactive response is no longer sufficient. It is becoming essential to adopt a proactive research approach capable of anticipating both technological developments and attackers’ strategies. In this context, innovation is emerging as a prerequisite for sovereignty, whether in post-quantum cryptography, trustworthy AI, or the security of embedded and distributed systems. CEA-List’s work is fully aligned with this dynamic, closely linked to industrial needs and emerging threats: anticipating to stay one step ahead.”

Marc OLIVIER
CEO

In the face of AI and the post-quantum era, bringing humans back into the loop

“ Generative AI, autonomous agents, and, in the future, post-quantum risk, are challenging the foundations of traditional authentication. When attacks can mimic, bypass, automate, and exploit on a massive scale, security can no longer rely solely on reusable credentials, codes, or secrets. The real challenge becomes proving conscious, contextualized human action. In sensitive environments, this shift is decisive: we need mechanisms capable of combining cybersecurity, sovereignty, traceability, and resilience against new threats. The future of digital trust will rely on models that validate intent, not just identity.”

Florin PAUN
Co-founder

All Xvaluators! : the cybersecurity of the future will be based on quality data or it won’t be at all!

“ In the current context of the proliferation of false or biased data (more than 60% of AI), a new AI typology in cognitive science (complementary to connective and symbolic approaches)–discovered by the founder of the French deep tech company Xvaluator (patent obtained in 2019) and recognized by the international scientific community for having complemented Condorcet’s Paradox and Arrow’s Theorem (including in the Springer Encyclopedia) enables (as embedded AI) the reduction of false data flows, the decrease of the ecological footprint, and the increase in the relevance of results from all AI tools and applications. This generic and sovereign French innovation enables effective consensus-based decision-making and the evolution of the digital business model from the current polarization toward “third-party-inclusive” approaches based on the relevance of qualified and qualifiable data within highly collaborative and democratic processes..”

Valérie DE SAINT PÈRE
President and Co-founder

In the face of the industrialization of threats, training cybersecurity talent differently

“ At a time when offensive AI, agent-based systems, and automation are redefining the threat, cybersecurity is shifting to a new scale: attacking is becoming industrialized, and defense must follow suit. In this context, École 2600 is fundamentally evolving its educational models and training professionals capable of working with and against these technologies. This involves anticipating which jobs are likely to disappear, integrating AI proficiency into the curriculum, and preparing students for more sophisticated malicious uses. True to its DNA, the school prioritizes an approach grounded in fundamentals–understanding before using–to ensure AI isn’t reduced to a mere productivity tool but is instead mastered as a field to better defend against threats. Training quickly is no longer enough; training must be precise and proactive.”

Cyrille VIGNON
CEO

Fighting AI with AI: sovereignty as an imperative

“ Generative AI has helped industrialize malware production: variants are created in a matter of hours, rendering traditional signatures obsolete. In the face of this acceleration, defenses must also evolve. Behavioral code analysis–understanding what a program does rather than what it looks like–is becoming essential for detecting unknown threats before they strike. But defensive AI is not enough: we must also master its foundations. Today, there is a strategic challenge: ensuring the sovereignty of our detection tools. Controlling one’s data, algorithms, and analysis infrastructure is no longer an option; it is an imperative for the European cyber ecosystem.”

Romain WALLER
Chief Executive Officer

In the face of the 2026 cyber threat, data sovereignty as a strategic pillar

“ In 2026, cyber threats reach an unprecedented level: state-sponsored attacks, industrialized cybercrime, and the massive exploitation of both human and technical vulnerabilities expose every organization, regardless of its size. In this context, data sovereignty becomes a major strategic issue. It guarantees not only control over information but also the ability to protect critical assets against increasingly sophisticated risks. The use of trusted, sovereign solutions designed to the highest security standards is essential. ERCOM solutions meet this requirement by ensuring confidentiality, integrity, and control. It is a choice of resilience, compliance, and digital independence. ”

FOCUS DOCAPOSTE-CYBLEX CYBERSECURITY BAROMETER 2025

DOCAPOSTE

Smara Lungu
Director of Strategy, Marketing, Communications, and Institutional Relations

"The gap is widening between the perception and reality of cyber risk: two-thirds of organizations report having suffered an attack, while two-thirds still downplay its scope. The third edition of our cybersecurity barometer, co-produced by Docaposte with Cyblex Consulting, confirms this. While basic measures are improving, governance weaknesses persist: prioritization of critical assets, organization of incident response, and the ability to make decisions under pressure. In a context of regulatory uncertainty, decision-making capacity weakens. Attacks-phishing (38%), ransomware (28%), data loss (17%)-exploit these vulnerabilities. Cybersecurity is becoming a direct business continuity issue, and its increasing prevalence fosters a false sense of control."

Docaposte-Cyblex Cybersecurity Barometer 2025

available at the following link:
urlr.me/nZYEG2

DOCAPOSTE CYBLEX Consulting

Cybersecurity Barometer 2025

The Cybersecurity Barometer, produced jointly by Docaposte and Cyblex Consulting, tracks year-on-year changes in the cybersecurity maturity of businesses and public sector organisations.

- **1/3 businesses suffered a cyberattack in 2025, just as they did in 2024.**

The most common cyberattacks:

- **38 %** Phishing
- **28 %** Ransomware
- **17 %** Theft/Loss of data

The consequences

- **24 %** System outages
- **21 %** Theft and/or loss of data
- **13 %** Production halted

- **50 % some organisations have successfully thwarted the attacks without any**

The safeguards put in place

- **89 %** Enhanced password management
- **85 %** Regular software updates
- **81%** Regular, outsourced data backup

+55 % cybersecurity budgets are on the rise (particularly in the public sector)

- **3/4** Some companies believe they are doing enough to protect themselves
- approx. **1/2** Companies tend to favour off-the-shelf solutions
- **1/3** of respondents are familiar with and follow the ANSSI guidelines

Sovereignty: essential in the public sector

- **55%** public sector stakeholders consider the use of sovereign systems to be very important

VS

- **37 %** private companies

5. CURRENT STATUS OF ONLINE THREATS
ACN Observatory of Digital Trust Sector 2026

6. MARKET TRENDS

6.1 General trends
- Focus: structuring the ecosystem to scale up – the role of the Cyber Campus
- Focus: overview of the Regional Cyber Campus Network

6.2 Regulatory trends
- Focus: the digital resilience index: a tool for measuring digital dependencies
- Focus: actions in the context of the AI Summit – February 2025

6.3 Technology trends
- Focus: research: programme agencies and cybersecurity

6.1 GENERAL TRENDS

1• The growth of the French sector

After the clear peak observed in 2022, growth in the French Digital Trust sector slowed for the third consecutive year. It stood at 5.4% in 2025, after 6.4% in 2024 and 6.8% in 2023, while remaining significantly above French GDP growth, which reached 0.9% in 2025. This slowdown does not call into question the sector's structural momentum, but it confirms its entry into a phase of more moderate growth, in a demand environment that is less favourable than in the aftermath of the 2021–2022 period.

This trend is primarily linked to the softening of historical segments. Digital Security grew by only 2.4% again in 2025, as in 2024, reflecting the slight slowdown in major identity, biometrics and access control projects that had strongly supported activity in 2022. Cybersecurity continues to grow, but in a less homogeneous way: cyber products remain on a relatively solid trajectory, with growth of 6.4% in 2025 after 7.8% in 2024, while cyber services slowed much more markedly, with growth of 3.4% in 2025 after 10.6% in 2024. This decline shows that the weaker economic conditions already affecting traditional IT services are now also impacting cyber services.

In this context, the most dynamic markets remain those where security requirements are the least discretionary: defence, space, security, major ministries and affiliated bodies, as well as banking and insurance. At the same time, some SMEs and intermediate-sized enterprises continue to record double-digit growth, showing that the slowdown observed at aggregate level does not affect the entire ecosystem uniformly, and that the players best positioned to address critical or differentiating needs continue to gain market share.

Thales' results clearly illustrate this phase of softening among some large historical players. In 2025, the group's Cyber & Digital segment declined by 0.9% organically, with the decrease notably linked to the commercial integration process of Imperva. At the same time, the figures published by Thales show a slight increase in digital identity on a like-for-like basis, confirming that traditional growth drivers remain present, but at a more moderate level than before.

By contrast, trusted AI now appears to be the sector's most dynamic segment: after already strong growth of 9.3% in 2024, it accelerated sharply to 23.4% in 2025. This dynamic contrasts clearly with the slowdown in more traditional segments and confirms that trusted AI is now one of the main drivers of expansion for Digital Trust in France, even though its economic weight remains lower than that of cybersecurity and Digital Security.

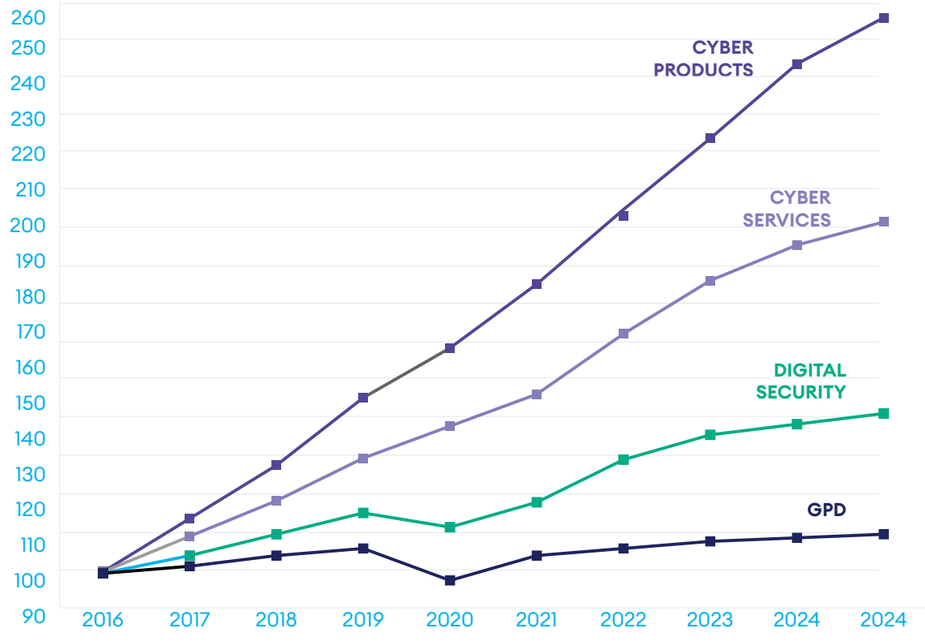
" The sector's overall growth rate is set to stabilise at around 5% in 2025 "

France growth comparison 2017-2025

Growth							
Segments	2019	2020	2021	2022	2023	2024	2025
Digital trust	8,5%	3,6%	7,3%	11,3%	6,8%	6,4%	5,4%
Cyber products	14,0%	10,9%	8,8%	12,6%	9,0%	7,2%	6,4%
Cyber services	10,3%	5,8%	8,9%	10,3%	9,4%	10,6%	3,4%
Digital Security	4,8%	-1,7%	5,2%	11,0%	3,8%	2,4%	2,4%
Trustworthy AI						9,3%	23,4%
GPD	1,8%	-7,8%	6,8%	2,5%	0,9%	1,1%	0,9%

The graph below shows the comparative growth of the three main segments of the Digital Trust industry and GDP over the 2017-2024 period.

Source : INSEE



Source : DECISION Etudes & Conseil

2• Markets in the industry

Markets in 2025

As shown in the diagram, the public sector in the broad sense, i.e. including health and transport, accounts for nearly one third of the French market, representing €6.8bn in 2025. The remaining two thirds come from the private sector, representing €13.7bn.
The private sector's influence is set to grow year by year. The digital trust sector actually emerged around the government and the need to secure Operators of Vital Importance (OVIs). The need for trust then extended to large companies in general, beyond OIVs. The current trend is now toward developing the market for small and micro-enterprises, most of which are ill-equipped to deal with the risk of cyberattacks that now affect them, particularly the risk of falling victim to ransomware.

Beyond the public sector, which remains the leading market and an important growth driver, the Banking / Finance / Insurance and Energy sectors have been the main drivers of the sector for more than three years, ahead of healthcare.

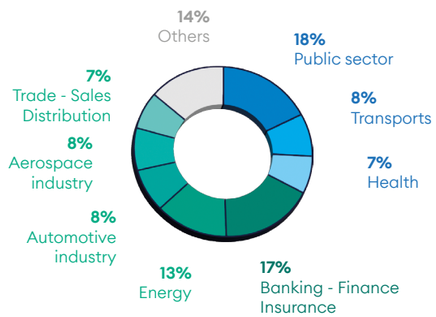
The emergence of a market for Micro-entreprise/SMEs and small local authorities

The series of diagrams opposite shows the segmentation of the French market by type of trust solution provider, distinguishing between large companies and SMEs / micro-enterprises.

The State, Operators of Vital Importance and large companies, excluding Operators of Vital Importance, account for more than 75% of the market served by the sector's large companies, and for 80% of their growth prospects in the coming years.

These large companies providing trust solutions account for 57% of the sector's revenue in France in 2025, or 77% if activities carried out outside France are included. This reflects the major traditional markets around which the sector was built: the State, Operators of Vital Importance and large private accounts.

Mains markets for the industry in 2025



Source : DECISION Etudes & Conseil, survey completed by companies in the sector between 2022 and 2026.
Responses are expressed as a percentage of respondents, weighted by their share of the sector.
The sample represents 12% of the sector's turnover.

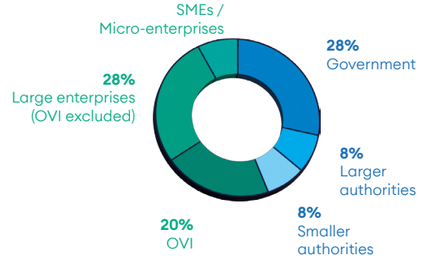
By contrast, the State and Operators of Vital Importance account for only 30% of the market served by the sector's SMEs and micro-enterprises. Large companies, at 31%, local authorities, at 23%, and SMEs / micro-enterprises, at 15%, represent most of the market and growth prospects for SMEs and micro-enterprises providing trust solutions in France. In other words, this view of the activity of the sector's SMEs and micro-enterprises highlights the emergence of two markets.

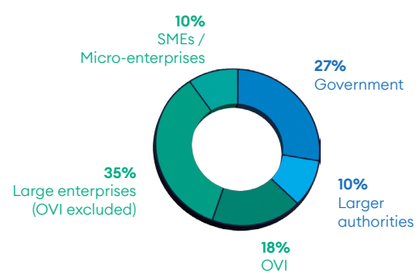
• The first is **the market for local authorities**, including small local authorities. By extrapolation, this market can be estimated at €3.9bn in 2025.
• The second, and above all the most important, is **the development of a market linked to the need for trust products and services among French SMEs and micro-enterprises**. By extrapolation, this market can be estimated at €2.3bn in 2025. It is characterised by dedicated offerings: standardised solutions, rapid deployment, low cost, and often no hardware component.The development of this market among French SMEs and micro-enterprises was slowed in 2020 by the COVID crisis. French SMEs and micro-enterprises were more affected by COVID-related restrictions than the traditional large customers of the Digital Trust sector, namely the State, Operators of Vital Importance and large companies, which are particularly focused on the provision of essential needs, including Banking / Finance / Insurance, Energy and Healthcare.

However, the structural trend is clearly towards the development of this SME and micro-enterprise market, which is set to become one of the sector's major markets and to underpin its growth in the coming years.

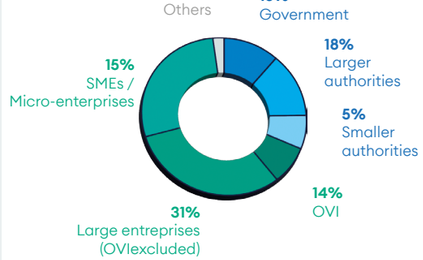
Finally, although they remain negligible for now, markets are beginning to emerge for securing associations and private individuals.

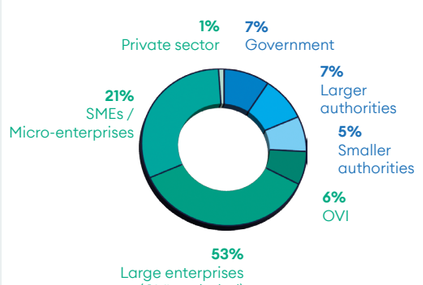
Large enterprise





Micro-enterprise





Source: DECISION Etudes & Conseil, survey completed by companies in the sector between 2022 and 2026.
Responses are expressed as a percentage of respondents, weighted by their share of the sector.
The sample represents 12% of the sector's turnover.

FOCUS STRUCTURING THE ECOSYSTEM TO SCALE UP – THE ROLE OF THE CAMPUS CYBER

CAMPUS CYBER

Joffrey Célestin-Urbain
Chairman

Farida Poulain
Executive Director

Has cybersecurity become a new issue of power?

«Cybersecurity has clearly changed in nature in recent years. Long considered as a technical matter related to the protection of information systems, it has now emerged as a strategic issue for governments, businesses, and citizens.

The digital transformation of economies, the rise in cyberattacks, and the emergence of transformative technologies such as artificial intelligence and quantum computing have profoundly altered the landscape of digital risks. At the same time, technological rivalries among major powers are placing digital infrastructure at the heart of issues related to economic security and strategic autonomy.

In this context, cybersecurity goes beyond the mere protection of systems. It plays a direct role in societal resilience, economic security, and the ability of states to control their technologies. It is now a pillar of digital sovereignty.
Campus Cyber is part of this dynamic, serving as a conduit for the national cybersecurity strategy and contributing to its operational implementation.**»**

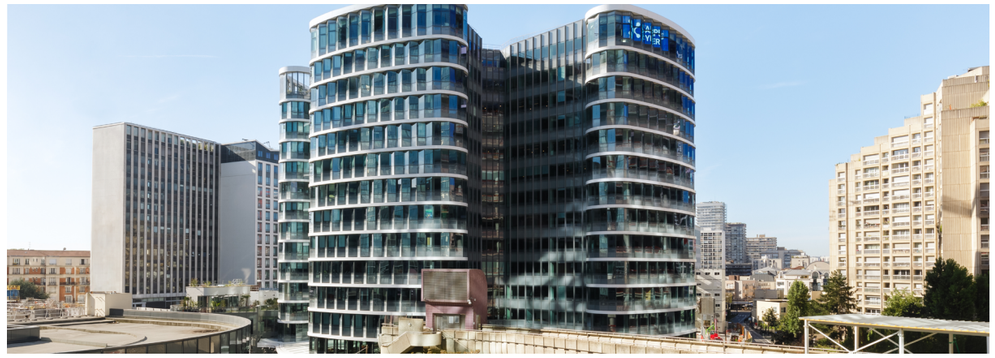
Precisely, what is your vision for the sector?

«At Campus Cyber, we see a rich but still fragmented European cyber ecosystem. Innovative startups, renowned research centers, and leading technology companies are developing some of the most advanced cybersecurity solutions. Yet a paradox persists. The talent exists. The technologies do too. But European companies still struggle to reach the critical mass that would allow them to fully compete with major international players.

Regulatory frameworks, procurement practices, and industrial dynamics remain largely organized at the national level. This fragmentation limits economies of scale and slows the emergence of players capable of making their mark on the international stage.

Added to this is the difficulty of accessing major clients. Many companies, particularly startups and SMEs, struggle to translate their innovation capacity into large-scale deployment.

In a sector where investments in research and development are substantial, speed to market becomes a decisive factor in competitiveness.**»**



What role does Campus Cyber intend to play in this context?

«Today, the challenge is no longer just to innovate, but to concretely organize the conditions for scaling up. It is precisely to address this challenge that Campus Cyber's 2026–2028 roadmap is being implemented. The Cyber Campus is not intended to replace existing players. It empowers them to work together, launch projects, test solutions, connect to the market, and move faster.

Its role is to organize collaborations, connect supply and demand more effectively, and foster the emergence of mechanisms that are useful for both the market and resilience.**»**

So the Campus Cyber is a player serving the ecosystem?

«That's exactly right ! The Campus brings together public and private forces in French cybersecurity and currently comprises 250 member entities, including 190 resident entities, covering the entire value chain: companies, public entities, research centers, training organizations, startups, and associations. This ecosystem includes, in particular, 110 member companies, 23 training organizations and schools, 5 research organizations, and 7 institutional stakeholders.

Following an initial phase dedicated to establishing the Campus and its community, the Campus is entering a new stage of its development. Its 2026–2028 strategy marks a turning point : transitioning from a gathering place to a key enabler, capable of organizing collective action and accelerating concrete projects.
This evolution directly addresses the need to transform a dynamic ecosystem into an operational one. It translates into a strengthened positioning as a service platform.

Specifically, the Campus offers operational tools to support stakeholders: networking, project development, access to testing grounds, and market connections.**»**

Can you give us a few examples?

«A first game changer will be the shared technical facility. It will enable testing of solutions, experimentation under real-world conditions, and validation of technologies prior to deployment.
We are also planning a growth incubator aimed at supporting cybersecurity startups and SMEs in their development by facilitating their access to clients, investors, industrial partners, and, where relevant, European partners.
The Campus also plays a key role in structuring demand by facilitating connections between solution providers and buyers, including large corporations, government agencies, and local authorities to promote large-scale deployment, particularly in light of the increasing regulatory requirements associated with the NIS2 Directive. This dynamic is reflected in particular by the development of a NIS2 services platform, aimed at guiding the organizations concerned, identifying their needs, and streamlining their access to suitable solutions.

In line with this approach to structuring and large-scale dissemination, Campus Cyber relies heavily on the rich network of French cybersecurity associations, whose initiatives, particularly those carried out within the framework of the ACN, actively contribute to raising awareness, providing training, and disseminating best practices.**»**

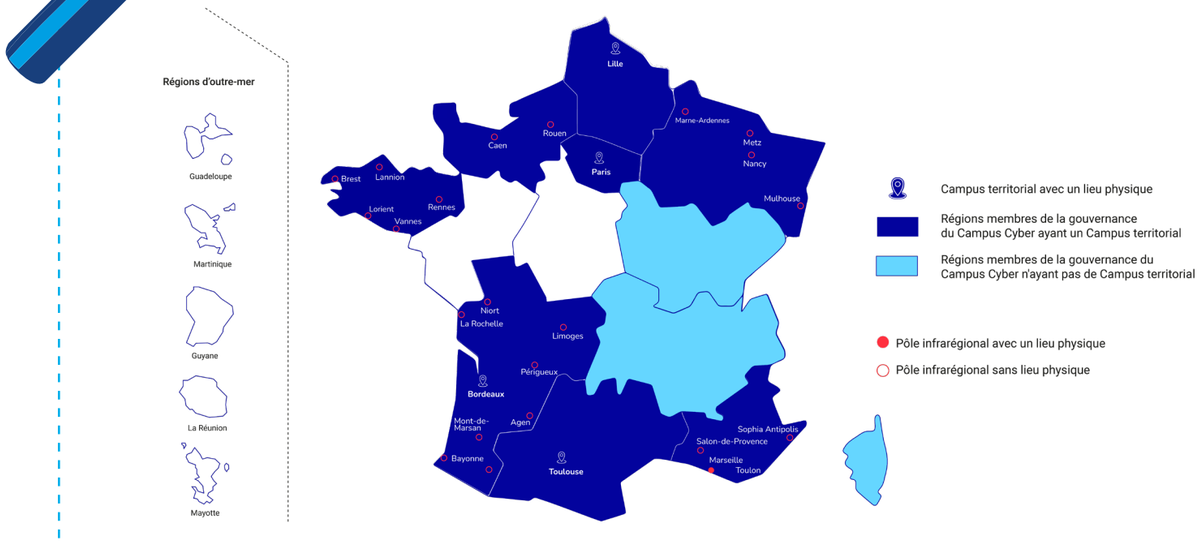
When we talk about scaling up, we naturally think of the international level—and, first and foremost, Europe?

«Indeed, and that constitutes a large part of our activities. We are developing an E2E (Ecosystem to Ecosystem) approach, which translates into concrete cooperation with other cybersecurity ecosystems : partnerships, project development, collaboration among stakeholders, and market access. The Campus has a clear ambition: to create the conditions for European stakeholders to collaborate and grow. However, this cannot be fully realized without a strong regional presence.

This is precisely the role of the network of regional Cyber Campuses, which enable this momentum to be deployed as close as possible to economic and public stakeholders, and ensure its operational implementation across the entire region.**»**

FOCUS

OVERVIEW OF THE REGIONAL CAMPUS CYBER NETWORK



Although indispensable and firmly established within their regional ecosystems, the Regional Cyber Campuses are still too often overlooked at the national level when it comes to their network structure, their missions, or their projects. This overview aims to address this gap and highlight opportunities for collaboration with each of the Regional Cyber Campuses.

Organization of the Network

«Initiated by the French government, the Campus Cyber is first and foremost a regional network through its network of regional Cyber Campuses. Since 2022, eleven metropolitan regions have joined the Campus Cyber initiative (Auvergne-Rhône-Alpes, Brittany, Burgundy-Franche-Comté, Corsica, Grand Est, Hauts-de-France, Île-de-France, Normandy, Nouvelle-Aquitaine, Occitanie, and Sud). Among them, eight have decided to create a regional Campus Cyber, and some are currently developing a pilot project (the Ile-de-France Campus is the national Campus Cyber).

The network of regional Campuses is managed through a dual governance structure. At the strategic level, the College of Regional Cyber Campuses is composed of regional councilors responsible for cybersecurity. It represents the network on the Board of Directors of the National Campus and serves as an interface with regional political bodies.

At the operational level, the network is led by the directors of the Campuses, who meet monthly to coordinate joint projects.»

Campuses that are all different...

«The Campus network is by nature a decentralized network, and no two Campuses are alike. Each region, based on its specific territorial characteristics and the maturity of its cybersecurity sector, is free to establish its own Campus in the most appropriate manner. Each Campus is legally independent from the National Campus and has its own human and financial resources.

Thus, the Campuses have different legal statuses (association under the 1901 law, SAS, or SEM). They may have a single physical location, subregional hubs, or be 100% virtual. Furthermore, each Campus specializes in themes historically aligned with its socio-economic fabric.

The Occitanie Campus naturally focuses on aerospace issues, while the Brittany, Normandy, and Southern Region Campuses are more involved in initiatives related to maritime and riverine challenges.»

“The aim is to foster the emergence and facilitate the consolidation of French and European cybersecurity leaders, in support of the European digital sovereignty agenda.”

...but very similar

«Beyond regional specificities, the Campuses are built on a common foundation. They all adhere to the shared principles outlined in the Cyber Campus Manifesto, the Network Charter, and the new three-year roadmap for the National Campus.

Moreover, in addition to the regional initiatives led by each Campus, they have decided to launch interregional initiatives that complement these efforts. This is the very purpose of the Campuses' joint roadmap, unveiled on April 1, 2026, during the InCyber Forum.»

The Campuses' Joint Roadmap

«The Campuses aim to meet a strong demand from cyber ecosystems: to provide easy access, anywhere in France, to a set of resources organized to meet the needs of all public and private stakeholders, whether in terms of protection, awareness, training, research, or procurement.

This is organized around two flagship projects, the foundations of which will be laid in 2026 and which will be rolled out nationwide starting in 2027:

• A service platform dedicated to supporting and equipping the stakeholders who are currently the least well-resourced and most vulnerable, particularly micro-enterprises, small and medium-sized enterprises (SMEs), and local authorities, many of which will fall within the scope of the European NIS II Directive, currently being transposed into French law.

• A nationwide incubator for innovative and technology-driven companies. The goal is to foster the emergence and facilitate the consolidation of French and European cybersecurity leaders, in support of the European digital sovereignty agenda. This will be achieved through the creation of a coherent and coordinated entrepreneurial pathway covering all phases of cybersecurity companies' growth.

The goal is to effectively implement the national cybersecurity strategy at the regional level, closely aligned with local realities, through a unified approach and a 'last-mile cybersecurity journey undertaken together' philosophy.»

• Nouvelle-Aquitaine Regional Cybersecurity and Digital Trust Campus

"Faced with an unstable digital environment and rising cybercrime, the Region has chosen to act proactively and through collective organization. The Nouvelle-Aquitaine Cyber Campus has established itself as the regional hub for digital trust. As an operational tool serving local communities, it protects SMEs, local governments, associations, and strategic sectors. It is developing a regional model for cybersecurity that supports economic development, the continuity of public services, and territorial sovereignty. Our vision: expertise at the local level. In the face of global threats, the response is local. We believe in human-centered cybersecurity that is accessible and locally rooted, capable of translating national policies into concrete actions. Supported by the Regional Council, the Campus Cyber Nouvelle-Aquitaine is recognized as a model for regional digital resilience, combining technical excellence, local solidarity, and cooperation with the State."

Mathieu Hazouard,
President of the Nouvelle-Aquitaine Regional Cybersecurity and Digital Trust Campus, Regional Councilor for Nouvelle-Aquitaine in charge of Digital Issues

Campus Director	Guy Flament	**CCT Location**	Pessac
Sub-regional hubs (if any)	Niort, La Rochelle, Limoges, Périgueux, Agen, Mont-de-Marsan, Pau et Bayonne (en création : Poitiers, Angoulême et Tulle)	**Website**	campuscyber-na.fr

Collaborative innovation at the heart of the Cyber Campus.
The Campus Cyber Nouvelle-Aquitaine stands out for its pragmatic and independent approach to digital defense, exemplified by pioneering open-source projects such as its Open-S -based SOC (Security Operations Center). This monitoring center, designed to be accessible and transparent, enables the sharing of detection tools without relying on costly proprietary solutions, thereby offering a robust alternative for public sector entities and SMEs.

At the same time, the Campus focuses on agility with the "Star-Hack" program, a one-of-a-kind educational bug bounty initiative. This program exposes students and young talent to real-world environments (in partnership with local companies) to identify vulnerabilities, thereby transforming cybersecurity education into an ethical and stimulating hands-on exercise.

This protection initiative is complemented by significant strategic support through its working group dedicated to the NIS2 Directive. This expert panel helps critical and important entities in the region anticipate new European regulatory requirements, thereby ensuring that the regional economic fabric remains compliant and resilient in the face of cyber threats.

By drawing on committed members such as Capgemini, Cheops Technology, and academic partners, the Campus does more than just monitor networks: it builds a genuine culture of shared security. This synergy between open tools, vulnerability detection, and regulatory compliance makes Nouvelle-Aquitaine a laboratory of excellence for digital trust.

• Campus Cyber Région Sud

Campus Liaison for the South Region	Pauline Sintes	**Campus Liaison for the South Region**	Marseille, Toulon, Sophia-Antipolis, Salon-de-Provence

The Campus Cyber Région Sud comprises four centres that drive the cyber ecosystem, working closely with the realities on the ground.

• Campus Cyber.ia Euromed

"Born from the vision of entrepreneurs and leaders, Campus Cyber.ia Euromed is perfectly aligned with the ambition of the national Campus Cyber network: providing an ecosystem of services to support businesses and local governments, promoting the sector and domestic expertise to enhance the region's cyber resilience. "

Pierre Boulogne,
President of Campus Cyber.ia Euromed

Executive Director	Clément Rossi	**CCT Location**	Marseille
Website	www.campuscyber-regionsud.fr		

Officially launched in November 2024, the Campus Cyber.ia Euromed supports and guides companies in their cybersecurity maturity and the deployment of secure and sovereign AI projects.

Co-founded by five committed local companies (Aix-Marseille Airport, CMA-CGM, CEPAC, FDJ United, Unitel Group), and located in the Euroméditerranée business district in Marseille, it features 2,000 square meters of space combining a cyber crisis management center, coworking areas, a modular event space, and offices. A true physical and digital platform connecting the local cyber and AI sector with demand (SMEs, mid-sized companies, and large enterprises), it has nearly 40 partner-members.

In 2025, nearly 60 events were organized at the Campus, including more than 100 participants spread across 9 crisis cells for the REMPAR25 exercise, making Euromed the top national site outside of the National Cyber Campus.

• Campus Sophia Antipolis

"Sophia Antipolis has always been a testing ground, a place where researchers, businesses, and institutions come together. With the Campus Cyber, we are taking a crucial new step: structuring, uniting, and expanding our ecosystem to foster the emergence of sovereign and competitive solutions in cybersecurity and artificial intelligence. This open-access campus reflects our way of working: flexible, collaborative, and deeply rooted in innovation. In the face of accelerating digital threats, our collective responsibility is to support businesses, protect citizens, and strengthen the resilience of our entire region."

Jean Leonetti,
President of the Sophia Antipolis Urban Community,
Mayor of Antibes-Juan-les-Pins

Directors	Jean-Pierre Mascarelli (C.A.S.A.) et Bernard Kleyhoff (Région Sud)	**CCT Location**	Sophia Antipolis

The Cyber Sophia Antipolis Campus is one of the pillars of the Southern Region's cybersecurity strategy. Located at the heart of Europe's leading technology park, it draws on a unique ecosystem bringing together more than 2,700 companies, 5,500 researchers, and 7,500 students, in an environment where digital technology, innovation, and research are deeply rooted.

Designed as an open campus, it brings together local strengths rather than centralizing them, mobilizing companies, laboratories, academic institutions, and public bodies around a shared ambition: to make Sophia Antipolis a national and international center of excellence in cybersecurity and artificial intelligence.

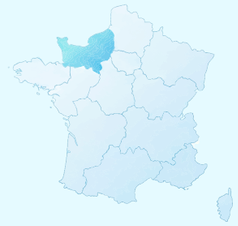
This unique approach is underpinned in particular by the presence of 3IA Côte d'Azur, the regional CSIRT, major research centers (INRIA, EURECOM, Université Côte d'Azur...) and major industrial players (Amadeus, Kyndryl, SAP Labs, Fortinet, Orange Cyberdefense, Thales...) that develop critical technologies in AI, data security, attack simulation, and automated threat detection.

Through its initiatives, the Cyber Campus supports the skill development of businesses, particularly micro-enterprises and SMEs, through awareness-raising, training, innovation, and incident response programs, while fostering cooperation between public and private sector stakeholders.

Supported by CASA and SYMISA, the campus is part of a transformative initiative for the region: integrated with the Alpha building (8,500 m^2), it will enhance the visibility and appeal of Sophia Antipolis by facilitating data sharing, managing digital risk, and fostering collaborative projects.

Through this networking initiative, Sophia Antipolis aims to serve as a catalyst for sovereign, competitive, and secure solutions that benefit businesses, citizens, and institutions.

• Campus Nomandie Cyber



"Certified as a 'Regional Cyber Campus' in May 2024, thereby becoming the fourth French Cyber Campus, Campus Normandie Cyber serves as the operational structure and resource center for implementing the 'Normandie Cyber' regional strategy ; it brings together businesses, higher education and research stakeholders, and local authorities around a shared ambition: to make Normandy one of the "regions of trust" for the digital security of small, medium, and mid-sized organizations and, more broadly, of the entire Normandy region. Since late 2025, it has been led by the Normandie Numérique association."

Stéphane Bresson,
Director of Campus Normandie Cyber

Campus Directors	Stéphane Bresson	**CCT Location**	Caen, Rouen
Website	www.normandie-numerique.fr		

The objective of Campus Normandie Cyber® is to raise awareness, support skill development, and enhance the maturity of all regional economic stakeholders (both beneficiaries and solution providers) while uniting and fostering the cybersecurity community.

It aims to transform cybersecurity threats into economic opportunities by developing the cybersecurity ecosystem and the market driven by these challenges. To meet these objectives, it fosters synergies within the regional ecosystem as well as with several other regional, national, European, and international ecosystems. It serves as a unifying hub for outreach, awareness-raising, and prevention initiatives.

Campus Normandie Cyber® facilitates the matching of supply and demand through local products and services within a marketplace. It relies on regional stakeholders who are both beneficiaries and providers.

Together with them, it offers several services that form the foundation of its service portfolio : regional CSIRT, DIH, incident and threat observatory, experimentation and innovation platform, engagement platform, and stakeholder and project qualification processes, among others.

While maintaining a generalist approach, it provides more specific support to certain sectors, notably the maritime and river transport sectors as well as industry.

• Cyber'Occ

"Protecting our microbusinesses, SMEs, associations, and local governments means protecting our entire economic and industrial fabric. It is a matter of competitiveness and survival, and Cyber'Occ was created precisely for this purpose. In 2025, we achieved decisive milestones, which will be continued and expanded in 2026. Our Cyber Campus in Labège in the Data Valley is now open ; the AMI-CMA Osmose project has begun rolling out its awareness and training initiatives ; and the incident response center (CSIRT), which can be reached at 0800711313, is fully operational. The Occitanie Region, under the presidency of Carole Delga, has taken on its responsibilities by creating Cyber'Occ. To build the regional resilience we need."

Marc Sztulman,
President of Cyber'Occ, Regional Councilor for Occitanie

Campus Director	Olivier Auradou	**CCT Location**	Labège
Website	www.cyberocc.com		

Amid growing demand for cybersecurity professionals, Cyber'Occ (Occitanie Regional Cybersecurity Center), designated as a regional Campus Cyber in November 2025, is actively engaged in structuring the training sector in the region.

As part of the OSMOSE consortium–a five-year project with €6 million in public funding led by the Universities of Toulouse and Montpellier–Cyber'Occ is contributing to the development of a cybersecurity skills observatory.

This tool is designed to map training needs at the regional level, identify labor market imbalances, and generate data to guide skills development policies. By aggregating information on sought-after profiles, available skill levels, and trends in cybersecurity professions, the observatory will provide training providers, companies, and public authorities with a shared and up-to-date view of the ecosystem.

OSMOSE brings together 21 academic, industrial, and institutional partners, including Airbus, Thales, and Aumovio, and offers a training program catering to an audience ranging from middle school students to professionals seeking career transitions.

Positioned at the heart of this consortium, Cyber'Occ serves as an interface between the academic world and the operational needs of regional companies.

Cyber'Occ thus establishes itself as the single point of entry for cybersecurity in Occitanie, with the ambition of making the region a national benchmark in training and digital sovereignty.

• Grand Est Cybersecurity Hub

"Since 2023, attacks against our local governments have surged by 400%. With the launch of the Grand Est Cybersecurity Hub, we are stepping up our efforts to better combat cyber threats together. Complementing our Grand Est Cybersecurity Assistance Center, this network of regional cyber Centers of Excellence enables us to raise awareness, provide training, and develop new solutions. It is by working together that we will make the Grand Est a trusted digital region."

Franck Leroy,
President of the Grand Est region

Campus Director	Kévin Sanna	**CCT Location**	Nancy, Marne-Ardennes, Mulhouse, Metz
Website	www.cybersecurite.grandest.fr		

The Hub is the Grand Est regional cybersecurity campus. Drawing on regional Centers of Excellence with specialized expertise, it works closely with stakeholders on the ground to bring together training, research, and innovation, develop skills, and strengthen digital sovereignty.

The Grand Est Region has adopted a unique approach: leveraging local talent and expertise spread across the region to build a strong, coordinated regional response.

The Grand Est Cybersecurity Hub thus becomes a true hub of convergence and innovation, a hub that is both large and accessible, where businesses, universities, institutions, and citizens can collaborate to strengthen our region's cybersecurity.

In a region characterized by high industrial density and rural areas, yet situated at the crossroads of Europe, the Grand Est Hub fosters cooperation among all stakeholders across different geographic levels and areas of expertise.

This cooperation makes cybersecurity more accessible, pools and deepens expertise, and serves collective resilience in the face of cyber threats.

• Bretagne Cyber Alliance

"With the Bretagne Cyber Alliance, Brittany has a tool at the service of its residents that will help project the influence of its entire cybersecurity ecosystem at the national and European levels to address today's major challenges."

Jérôme Tré-Hardy,
President of the Bretagne Cyber Alliance, Regional Councilor for Brittany

Campus Director	Tiphaine Leduc	**Website**	www.cyberalliance.bzh

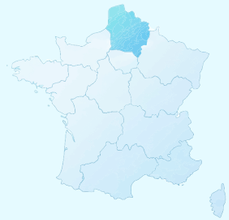
The Campus Cyber Breton, Bretagne Cyber Alliance, was born out of the collective desire of the Region and five Breton territories (Brest Métropole, Rennes Métropole, Lannion Communauté, Lorient Agglo, Vannes Agglo) to take action to develop a major regional sector and contribute to the protection of economic sectors as well as society as a whole.

The Campus Cyber Breton, which brings together the academic community, training providers, economic development stakeholders, and businesses, is committed to activating and energizing the cyber community, fostering interactions among the sector's various stakeholders, and promoting the Breton cyber ecosystem as a benchmark in France and Europe for a safer digital world.

Bretagne Cyber Alliance structures its activities around four missions :
• Supporting the growth of cybersecurity industry players
• Strengthening research and innovation performance
• Promoting a culture of cybersecurity throughout society
• Addressing skills needs

Bretagne Cyber Alliance produces resources made available to the community of pure-play cyber companies and the sectors requiring security :
• The Cybersecurity Maturity Barometer, a key tool for measuring, managing, and accelerating the cybersecurity maturity of businesses and local governments. With 400 respondents, it serves as a true compass for securing these stakeholders.
• The NIS 2 Observatory identifies targets subject to NIS 2 within the region' territory. It is a tool that helps anticipate and support stakeholders affected by the upcoming directive.
• The map of available funding identifies and summarizes the funding available at the European, national, and regional levels to help organizations launch a security initiative.
• The directory of regional cybersecurity stakeholders helps identify providers, solutions, and services that protect and secure systems.
• The training offerings catalog : with 120 training institutions, the training offerings are particularly diverse and cover the entire value chain of cybersecurity skills.

• Hauts-de-France Lille Métropole Cyber Campus



Campus Director	Chekib Gharbi	**CCT Location**	Lille
Website	hdf.campuscyber.fr		

The Hauts-de-France Lille Métropole Cyber Campus has established itself as a key player in cybersecurity in the region, bringing together nearly 150 companies, including recognized leaders such as Advens and Vade-Hornetsecurity. Its mission is clear: to strengthen the region's digital resilience by combining training, innovation, and support for economic stakeholders.

This Cyber Campus stands out in particular for two key features: first, an immersive training program based on a cyber range that enables realistic scenarios (CTF, crisis management); and second, the development of an entrepreneurial ecosystem, with a dedicated incubator supporting some thirty cybersecurity startups.

Positioned at the intersection of public and private interests, it hosts the ComCyber-MI's CNF Cyber, reinforcing its strategic role at the national level.

Among its key objectives, this Cyber Campus aims to accelerate the technological intensity of regional cyber companies. As part of this effort, it leads foundational projects such as a cyber POC program funded by the EDIH, enabling companies to test innovative solutions under real-world conditions.

A long-standing partner of the InCyber Forum, it has also developed the Campus Cyber Summit, which has become a leading event for industry professionals.
Thus, the Hauts-de-France Cyber Campus-- Lille Métropole serves as a unique platform where expertise, innovation, and economic development converge to benefit the region.
The Campus is a business unit of Euratechnology.

6.2 REGULATORY TRENDS

1• Europe : Towards a Trusted Digital Single Market

The digital transformation continues to unfold in Europe against a geopolitical backdrop marked by growing tensions and an escalating threat. Faced with these challenges, the establishment of a trusted digital single market applicable throughout the European Union has become a priority for all stakeholders in the sector. New risks associated with emerging digital uses are prompting European institutions and Member States to adapt their legislative frameworks to better control their technological future and strengthen their strategic autonomy.

In this increasingly competitive digital landscape, where China and the United States are vying for technological dominance, Europe must position itself as a resilient, innovative, and indispensable global player. It is with this in mind that the “For a Digital Europe” program was designed: it aims to make Europe a major player in the digital sphere, strengthen its technological sovereignty, and ensure its resilience amid growing tensions in cyberspace.

In fact, the year 2025 marked a decisive turning point in this dynamic, with the concrete entry into force of several landmark regulations, such as DORA (Digital Operational Resilience Act) and REC (Resilience of Critical Entities). Indeed, supplier risk management and supply chain resilience are becoming priorities. Organizations must now evaluate their partners not only on technical criteria, but also on their compliance with European requirements and their ability to guarantee data sovereignty.

All of these efforts are priorities for the digital trust sector. Like 2025, 2026 is a pivotal year from an institutional perspective in Europe. In partnership with its German counterpart Teletrust, the ACN published its European priorities and recommendations in April 2024 to accelerate the transition toward a trusted digital single market and was sure to share them with all Members of the European Parliament. ACN aims to build on the success of this cooperation with its German counterparts to expand it and seeks to establish partnerships with representatives of the digital trust sector in several other European countries. The goal of this cooperation among inter-European sector representatives is to get to know one another better and to develop common messages to convey them with greater impact.

ACN document “Digital trust industry priorities for the 2024 European elections”

available at the following link:
urlr.me/rwy7zJ

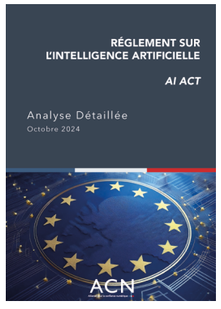
The Implementation of an Interoperable European Digital Identity

The revision of the “Electronic Identification, Authentication, and Trust Services” (eIDAS) Regulation, aimed at implementing a secure and interoperable digital identity in Europe, was finalized on April 30, 2024, with its publication in the Official Journal of the European Union. Europe is therefore on the verge of enabling all its residents to have a personal digital wallet usable throughout its territory (EUDI Wallet). Its implementation will be based on common technical standards (Architecture and Reference Framework – ARF), which are still under discussion. Starting in 2027, Member States will be required to provide every European citizen with a digital identity wallet free of charge.

Additionally, **a draft regulation on “European Business Wallets” was published by the European Commission on November 19, 2025, as part of the Digital Omnibus package.**
The Business Wallet is a solution designed to reduce administrative burdens and enable businesses and public sector organizations to identify, authenticate, and exchange data securely, with legal validity throughout the European Union. This initiative will be accessible to businesses of all sizes (micro-enterprises, SMEs, mid-sized companies, large enterprises) as well as public administrations. This wallet will enable: identity verification of counterparties, the creation and storage of trusted documents (permits, licenses, certificates), digital signatures, and simplified communication between businesses and between public administrations. While businesses are not required to adopt this wallet, the Commission highlights substantial benefits in terms of administrative simplification, security, interoperability, and economic growth. **Following the adoption of this business wallet by the European Parliament and the Council of the EU, all levels of government in the Member States will have two years to implement the business wallet.**

Establishing a European Legal Framework for Artificial Intelligence

The Artificial Intelligence Regulation (AI Act) was published in the Official Journal of the EU on July 12, 2024, and entered into force on August 1, 2024. The first applicable provisions concern the prohibition of AI systems posing an unacceptable risk, as well as transparency obligations for general-purpose AI models. Starting August 2, 2026, all organizational, technical, and documentation requirements for high-risk systems will become mandatory. Products incorporating high-risk AI systems are granted an additional grace period, with enforcement postponed until August 2027. This phased timeline allows companies to adapt, but it requires an acceleration of compliance programs, particularly for regulated sectors and critical infrastructure.



ACN Report: “Detailed Analysis of the Artificial Intelligence Regulation – AI ACT”

available at the following link:
urlr.me/SJU2sj

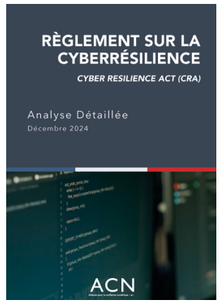
Strengthening Cybersecurity

CRA

The Cyber Resilience Act (CRA) was published in the Official Journal of the European Union on November 20, 2024, and entered into force on December 10, 2024. The Cyber Resilience Act (CRA) aims to establish common European cybersecurity standards for products to be placed on the European internal market. This seeks to strengthen the responsibility of manufacturers and suppliers of products containing digital components by requiring the implementation of adequate cybersecurity safeguards. This regulation applies to all products containing digital components and ancillary services, including hardware and software (regardless of the manufacturer's size). However, the regulation will not apply if the products are not intended for commercial use or if they are already covered by other legislation.

The implementation of the CRA will be phased: 18 months after the CRA enters into force, assessment bodies will be authorized to verify product compliance. As of September 11, 2026, manufacturers will be required to report exploited vulnerabilities in their products to ENISA. Full implementation of the regulation is set for December 11, 2027. Thus, all CRA requirements will apply, including pre-market minimum standards, vulnerability management, and the duty of transparency toward users.

In this regard, ACN is stepping up its information and awareness-raising efforts among industry stakeholders so that they can anticipate and prepare for the gradual implementation of the CRA.



ACN report "Detailed analysis - Cyber Resilience ACT"

available at the following link:
urlr.me/urQveD

• ACN webinar on the Cyber Resilience Act (CRA) in December 2025

As part of the implementation of the European Cyber Resilience Act (CRA) regulation, the ACN organized an awareness-raising webinar in December 2025, with the participation of institutional, industry, and legal stakeholders to address the CRA from various perspectives.

This event provided members with an opportunity to learn about the challenges of the CRA, its obligations, its implementation, and how to prepare for it. It serves as a reminder that compliance with the CRA should not be viewed solely as a burden for businesses but as an opportunity to position themselves as trusted actors within the ecosystem.

The interest shown by members in this ACN event underscored the importance of making the CRA accessible and understandable to all stakeholders, and thereby ensuring the long-term viability of the digital trust ecosystem.

• Organization of the ACN Cybersecurity Certification Conference (ACCC) in February 2026

As part of the fourth edition of the ACN Cybersecurity Certification Conference (ACCC), organized by ACN in February 2026, we were pleased to welcome the European Commission, ANSSI, and ENISA to discuss strategic issues related to certification and standardization, with a particular focus on the implementation of the CRA for companies in the sector..

Thanks to the high-quality contributions from public institutions and industry experts, the ACCC provided a forum rich in discussion and practical recommendations for the sector. Discussions focused in particular on the various European certification schemes and ways to prepare for the requirements of the CRA.

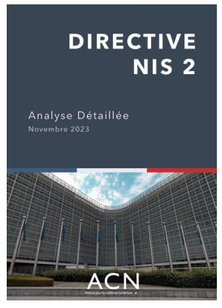
Furthermore, the ACCC provided concrete pathways to help companies in the sector achieve compliance while strengthening their competitiveness and innovation.

Cyber Solidarity Act

Furthermore, in light of growing cybersecurity risks, efforts to strengthen European solidarity in this area have also been addressed through legislation in the form of the Cyber Solidarity Act, aimed at establishing a “European cyber shield”–a cyber emergency mechanism–which includes the creation of a “European Cyber Reserve” and a mechanism for analyzing cybersecurity incidents. Following a trilogue that reduced the original budget allocated to the European Cyber Reserve, the text was adopted by the Council of the EU on December 2, 2024, along with the accompanying amendment to the European Cybersecurity Act. It entered into force on February 4, 2025.

NIS 2

The European Commission published the NIS 2 Directive, a revision of the NIS Directive, in the Official Journal of the European Union on December 27, 2022, and it entered into force on January 17, 2023. The measures implemented by the NIS 2 Directive are intended to ensure a high common level of cybersecurity across the European Union. It aims to ensure a trustworthy cyberspace for citizens and businesses and to strengthen cooperation among Member States. The text of the directive is currently under review and being transposed into French national law (see p.102 draft law on the resilience of critical infrastructure and the strengthening of cybersecurity).

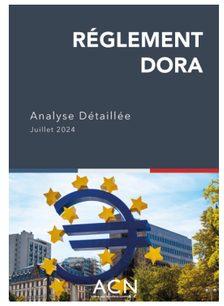


ACN report “detailed analysis of NIS 2 directive”

available at the following link:
urlr.me/VWAHzj

Digital operational resilience in the financial sector

The Digital Operational Resilience Regulation (DORA) and the associated directive entered into force on January 16, 2023. DORA sets out uniform requirements to strengthen and harmonize the management of risks related to information and communication technologies (ICT) and the security of networks and information systems at the EU level. It also provides for the establishment of a mechanism for the direct supervision of critical ICT service providers at the EU level.



ACN report “Detailed analysis of the DORA regulation”

available at the following link:
urlr.me/9M2Ubf

Toward Simplifying and Streamlining the Regulatory Framework – Digital Omnibus

In response to the growing complexity of this “digital patchwork,” the European Commission launched the Digital Omnibus package on November 19, 2025. This initiative aims to simplify and clarify the rules governing artificial intelligence, data, and cybersecurity, in order to reduce overlaps between different regulations (CRA, NIS 2, DORA) and facilitate compliance for micro-enterprises and SMEs.

Among the flagship initiatives is the creation of EU-wide “regulatory sandboxes.” These environments allow innovators to test their solutions in a controlled setting without fear of immediate penalties for non-compliance. This approach aims to encourage innovation while ensuring a high level of data protection and security.

The European Commission is also working to harmonize certification and audit procedures in order to reduce costs and lead times for businesses. The goal is to transform regulatory constraints into drivers of growth by fostering the emergence of European champions in the fields of trustworthy AI, sovereign cloud, and cybersecurity.

2• National Initiatives on Digital Trust

Draft Law on the Resilience of Critical Infrastructure and the Strengthening of Cybersecurity (Transposition of REC-NIS2-DORA))

On October 15, 2024, during the Council of Ministers, the Minister of the Economy, Finance, and Industry, the Minister of Higher Education and Research, and the Secretary of State to the Minister of Higher Education and Research, responsible for Artificial Intelligence and Digital Affairs, presented the bill on the resilience of critical infrastructure and the strengthening of cybersecurity, which transposes the NIS 2 Directive into French law, as well as the REC and DORA texts.

As part of a special committee tasked with reviewing the bill, the ACN was heard by Senator Olivier Cadic, Chair of the Special Cybersecurity Committee, and Senators Hugues Saury, Patric Chaize, and Michel Canevet, rapporteurs on the bill regarding the resilience of critical infrastructure and the strengthening of cybersecurity.

The ACN welcomes the coherent integration of the GDPR/NIS2/DORA texts into a single bill, which enhances the clarity and understanding of the requirements for strengthening national security and resilience. It calls for rapid transposition and implementation to address the challenges of collective resilience and strategic autonomy, while supporting the French digital trust ecosystem. The ACN emphasizes the need for extensive support (communication, training, best practices) for regulated entities, which are often new to cybersecurity. A cybersecurity tax credit and European grants have been proposed to offset costs, particularly for micro-enterprises and SMEs, and to avoid the economic risks associated with inaction. Finally, it was suggested to create an association to monitor the effectiveness of the decrees and to incorporate additional measures: consideration of the human factor, a vulnerability disclosure policy, and a legislative framework for OSINT.

The transposition of the NIS 2 Directive has been delayed due to political instability in France. The National Assembly's special committee met in early September 2025 during the extraordinary session and submitted the text at the conclusion of the session. It is expected to be examined in a public session of the National Assembly during the first half of 2026, before continuing its legislative process and being incorporated into French law.

Meanwhile, pending the publication of all transposition texts, ANSSI published a NIS 2 cybersecurity framework titled "ReCyF" in March 2026. This framework aims to prepare entities for compliance with NIS 2 and, more specifically, to strengthen their security posture in the context of a constant cyber threat.

The 2026–2030 National Cybersecurity Strategy

The 2026–2030 National Cybersecurity Strategy was presented on January 29, 2026, by Anne Le Hénanff, Minister Delegate for Artificial Intelligence and Digital Affairs, and is based on five structural pillars, broken down into fourteen strategic objectives.

The first pillar, "making France the largest pool of cybersecurity talent in Europe," aims to develop the cybersecurity workforce and talent ecosystem in France. This involves investing heavily to steer young people toward these careers from an early age and supporting training and recruitment initiatives in this field.

The second pillar, "strengthening the nation's cyber resilience," focuses on raising the overall level of cybersecurity among all economic and social actors. This plan will rely on enhanced synergy between the State, local authorities, businesses, research institutions, and civil society.
The third pillar, "curbing the spread of cyber threats," is dedicated to combating cybercrime, with increased resources for ANSSI, the police, and specialized judicial bodies, and a central role assigned to the Cyber Risk Coordination Center (C4) to mobilize response mechanisms against cyberattacks, in collaboration with all state actors. Measures to protect against cyberattacks will be established in close collaboration with private-sector actors.

The fourth pillar, "maintaining control over the security of our digital foundations," aims to reduce technological dependencies by supporting the consolidation and advancement of the cybersecurity sector. This pillar will rely on continued government investment in cybersecurity under the France 2030 plan and on enhanced dialogue among stakeholders.

The fifth pillar, "supporting the security and stability of cyberspace in Europe and internationally," aims to develop European and international cyber defense across three spheres of action : the EU, NATO, and beyond, by fostering cooperation with partners who share common interests in cyber defense.

Publication of the SGDSN's "National Cybersecurity Strategy 2026–2030"

available at the following link:
urlr.me/mnAY3q

The National Strategy to Combat Information Manipulation 2026–2030

The National Information Warfare Strategy, published in February 2026 by the General Secretariat for Defence and National Security, is structured around four pillars, which are broken down into fifteen strategic objectives.

The first pillar, 'Mobilising the Nation to Strengthen Resilience', aims to educate and raise awareness among French society with a view to developing a collective culture of vigilance against information manipulation. These themes will be incorporated into the school curriculum and during citizenship days (JDC, Civic Service). In addition, the Academy for Combating Information Manipulation (LMI) will be established, under the auspices of VIGINUM.

The second pillar, 'Regulating online platforms and generative artificial intelligence services', is dedicated to strengthening the regulation of digital platforms and generative AI in order to limit systemic risks of manipulation, with rigorous implementation of the European Digital Services Act (DAS).

The third pillar, 'Strengthening national operational capacity to combat foreign digital interference', aims to improve the State's operational capacity to detect and counter foreign digital interference by consolidating a permanent monitoring mechanism (COLMI) and establishing an interministerial response strategy. Particular attention is paid to strengthening judicial capacities, particularly during election periods, in order to ensure a rapid response to attempts at manipulation. Objective twelve of this pillar specifically addresses support for the emergence of a sovereign open-source intelligence (OSINT) sector. The idea is to combine an ecosystem of tools, skills and public-private cooperation, whilst supporting the independent community of analysts.

The fourth pillar, 'Ensuring a free, open and secure information space through a multilateral approach', aims to build international cooperation to guarantee a secure information space. It provides for the establishment of a European community to combat manipulation and support for vulnerable states and regions.

Publication of the SGDSN's "National Strategy to Combat Information Manipulation 2026–2030"

available at the following link:
urlr.me/UGbunw

FOCUS

THE DIGITAL RESILIENCE INDEX: A TOOL FOR MEASURING DIGITAL DEPENDENCIES

Digital Resilience: A Strategic Priority for Organizations

Digital transformation brings with it a growing dependence on technologies, suppliers, and infrastructures.

This trend results in a gradual loss of control over information systems, increased complexity, and interdependencies that are becoming increasingly difficult to grasp: a significant and growing portion of European digital spending is directed toward non-European technologies (€265 billion in 2025).

At the same time, fewer than 10% of organizations objectively assess their technological dependencies, even though these dependencies determine their ability to manage risks, costs, and strategic autonomy.

In this context, digital resilience is becoming a central issue, at the intersection of sovereignty, performance, and business continuity.

The Digital Resilience Index: A Structured Approach

The Digital Resilience Index (IRN) was designed to address this need for visibility and management. It is a common framework for measuring and objectively assessing organizations digital dependencies based on their critical systems and processes.

The approach is based on several key steps:

- **Identify** an organization's most critical processes
- **Measuring** dependencies through the analysis of the applications and technological assets of these processes
- **Identify** areas of vulnerability through dependency mapping
- **Make decisions** by objectively evaluating strategic trade-offs
- **Transform** by implementing remediation and IT system evolution plans

The IRN offers a "full stack" approach, covering all dimensions of resilience (technological, operational, data, cyber, legal, supply chain, etc.), and is based on an open standard that is shareable and comparable across organizations.

It is designed to integrate existing risk management and compliance frameworks (such as NIS2, DORA, or ISO standards), complementing them with an approach centered on the analysis of digital dependencies and their strategic management.

Driven by an ecosystem of public and private stakeholders, the initiative aims to establish a common language and a reference framework for managing digital resilience at the enterprise and sector levels.

Structured support for organizations

Driven by an ecosystem of public and private stakeholders, the initiative aims to establish a common language and a reference framework for managing digital resilience at the enterprise and sector levels.

- Accredited firms that validate the ability of certified companies to carry out their missions.
- Approved companies that conduct assessments and can certify the level of digital resilience of user companies.

Within this framework, a structured support model is being implemented. Organizations can adopt the framework independently or receive support from accredited stakeholders authorized to conduct assessments and assist with the certification process.

This framework aims to create a market for qualified expertise in digital resilience, based on a common, open, and shared standard. It also ensures consistency in practices, comparability of results, and the gradual maturation of organizations, regardless of their size or sector:

The IRN thus serves the public interest: beyond being a diagnostic tool, it establishes a common language between executive management, IT departments, and risk functions, and acts as a lever for managing the information system as a strategic asset.

- **Provision of the framework** and assessment methods to enable each company to conduct its own self-assessment,

- **Accreditation and Certification** – H2 2026

The IRN will be deployed in companies through a network of accredited and certified firms:
  o Accredited companies (by aDRI) approve companies that will be able to work on the IRN with their clients,
  o Approved companies conduct assessments and can certify the level of digital resilience of user companies,

- **Communication and promotion** of the IRN label.

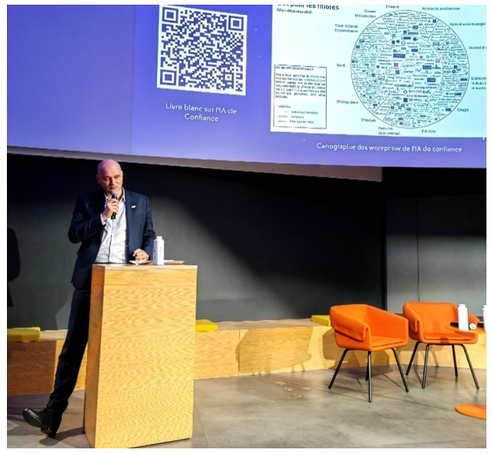
"The IRN initiative is designed to rely on an ecosystem of certified stakeholders capable of supporting organizations in analyzing their dependencies and implementing their resilience roadmap. As a long-standing partner of the project, Docaposte will be among the companies authorized to provide this support, alongside other accredited stakeholders"

FOCUS

ACTIONS IN THE CONTEXT OF THE AI SUMMIT – FEBRUARY 2025

The Global AI Summit, held in New Delhi from February 10 to 12, 2026, under the joint presidency of India and France, brought together more than 120 countries, as well as thousands of industry leaders, academics, and civil society representatives. The goal was to promote useful AI tailored to local contexts, serving the public interest and supporting the achievement of the Sustainable Development Goals. The summit also provided an opportunity to review progress on initiatives launched at the previous summit, held in Paris in February 2025, where the foundations for global governance of trustworthy AI were laid.
In this context, the second edition of the Rencontres de l'IA de Confiance (RIAC) took place on 27 January 2026 at Campus Cyber, and was accredited as part of the AI Impact Summit in New Delhi.

Anne Le Hénanff - Minister for Artificial Intelligence and the Digital Affairs



Grégory Wintrebert
ACN Chairman

Guillaume Poupard
Co-Chair of the National Council for AI and Digital Technology

This event brought together public, private, and institutional stakeholders to discuss the concept of trust in AI-related issues. On this occasion, Anne Le Hénanff, Minister Delegate for Artificial Intelligence and Digital Affairs, reaffirmed the government's commitment to trustworthy AI, highlighting its key role in France's innovation and competitiveness. At the same time, the Minister highlighted the vital role of the ACN in representing and structuring this sector.

The event aimed to explore the role of institutions in implementing reliable AI and the economic levers for developing a robust industrial ecosystem for trustworthy AI. It provided an opportunity for government agencies (ANSSI, DGE, CNIL), industry players (Docaposte, Safran.AI, etc.), and academia to exchange perspectives during two roundtables, while concrete use cases illustrated the operational application of trustworthy AI in industry.

The discussions confirmed that trusted AI is a strategic priority for France and Europe as a driver of innovation and economic growth.

ACN White Paper: "Trustworthy Artificial Intelligence"

available at the following link:
urlr.me/Kr6S4J

6. MARKET TRENDS
ACN Observatory of Digital Trust Sector 2026

ACN Publishes White Paper on Blockchain

On may 2026, ACN published a white paper on blockchain aimed at the general public. This document aims to highlight the presence of blockchain and the markets in which it operates. This white paper explores blockchain as a strategic pillar for the digital economy by analyzing the strategic, economic, and operational challenges associated with blockchain technology. It provides an overview of blockchain markets, the challenges of digital sovereignty for France and Europe, as well as concrete use cases for blockchain.

ACN White Paper : "Blockchain"

available at the following link:
www.confiance-numerique.fr/publications/

ACN Publishes a Report on the Mapping of Safety Standards

On may 2026, the NORSEC Commission of the CSF IS, a forum for discussing standardization issues within the ACN, began drafting a report with the aim of mapping: standardization challenges, the various standardization bodies, and the standards associated with each of them in the field of safety.

The deliverable, "Overview of Safety and Security Standards," is intended for everyday users of standards, public authorities, and economic stakeholders, with the goal of promoting standardization for its strategic characteristics and advantages. The aim is to support collective resilience, with a view to creating a safer, more sovereign, and more resilient environment.

"Overview of Safety and Security Standards"

available at the following link:
www.confiance-numerique.fr/publications/

6.3 TECHNOLOGY TRENDS

Technological innovation has been the main driver of growth in French and global Digital Trust for more than 10 years and this trend is expected to continue at least for the next 10 years. Technological developments affect Digital Trust in different and complementary ways.

1• Electronic and digital innovations that generate new markets

Innovations in the electronic and digital industries are impacting almost all sectors of modern economies and are thus generating new markets for Digital Trust.

• **Electronic systems and components are characterized by miniaturization and lower costs.** This trend, epitomized by Moore's Law, has shaped the global economy for the past 50 years, and is set to continue for at least the next decade, with the development of multilayer 3D memories and the miniaturization of processors. However, this trend is coming to an end. Investments to continue Moore's Law and keep pace with innovation are growing exponentially, and have already reached such levels that only seven companies are holding their own worldwide: Samsung (South Korea), TSMC (Taiwan) and Intel (USA) in processors, and Samsung (South Korea), SK Hynix (South Korea), Micron (USA), Western Digital (USA) and Toshiba (Japan) in memories. Today, however, there are alternatives to the development of Moore's Law, such as advanced packaging and heterogeneous integration, which are seen as alternatives to the production of increasingly high-performance chips at lower investment cost.

As a result of miniaturisation and falling costs, electronic products are becoming more democratic, including digital trust: sensors, tracking and tracing systems, and all the sub-systems included in the electronic segments of the industry.
This is a long-term phenomenon. In the short term, the growth of electronic components is cyclical and the 2020-2022 period was instead marked by surge in semiconductor prices. Since the beginning of 2023, the decline in semiconductor prices has resumed its course.
Over the next five years, only increases in energy prices are likely to counterbalance the price decline associated with the further miniaturisation of electronics, depending on the magnitude of these increases, particularly in Europe.

• **Digital transformation,** i.e. the digitalisation of tools, products and services in all sectors of the economy. This digitalisation process is still in its beginnings on a global scale. It is leading to an ever-increasing share of digital issues and this trend is expected to last for at least the next 20 years through the deployment of the Cloud-to-Edge continuum and its outlets in industrial IoT (embedded software, connectivity, cloud).

The intersection of these two trends is generating many emerging and promising markets for digital trust.

1. Security of connected objects

Eventually, if every object becomes connected, every object will need a cyber tool to secure it. Moreover, the interconnection of connected objects increases the cybersecurity risks by making entire networks vulnerable. Consequently, the interconnection of objects represents a huge growth potential for the associated cybersecurity products and services: identification and authentication of IoTs, secure elements, security of communications (5G / 6G, long-distance IoT communication protocols such as LoRa and Sigfox or short-range protocols such as Wi-Fi, Z-Wave, Bluetooth Low Energy, etc.), infrastructures, applications (hypervisors, etc.). Until now, the growth resulting from connected objects has not yet impacted the French security industry, although many of them have already been working on a dedicated offer for several years. Progress in the standardisation and interoperability of IoT architectures is likely to accelerate future growth.

• **Connected car.** The main segment, which is already growing strongly, is that of securing cars and their communications: Vehicle-to-Vehicle (V2V), Vehicle-to-Infrastructure (V2I: toll, etc.), Vehicle-to-Device (V2D: smartphone, etc.).

• ***Smart & Safe City.*** The development of connected objects in cities for security purposes is the second segment that has generated the most significant growth worldwide among digital security and cybersecurity players in connected objects since 2015. The players that have benefited most from the Safe City theme are the major integrators (Thales, Accenture, Capgemini, etc.). Safe City is generally less successful in France than abroad (whether in China, the United States or in many emerging countries) for three main reasons: the French administration, which was built around non-digital processes, the great diversity of public players in France (central state, regions, departments, municipalities, communities of municipalities, etc.), and budgetary austerity.

• **Securing Industry 4.0.** The growth associated with the deployment and securing of Industry 4.0 is expected to be increasingly felt over the coming years. However, installing connected objects inside a factory does not necessarily require the development of dedicated connected object solutions from cyber suppliers as the objects can all be connected to the central factory server. In other words, the classic and slightly older IT-OT technology is sufficient. As a result, the development of connected objects in Factory 4.0 does not result in a significant increase in orders for the implementation of specific solutions for securing connected objects in these factories.
France has major players in all the security segments associated with securing IoTs, but lacks national players of significant size for the deployment of service platforms associated with connected objects (of the type of GAFAMI in the USA or BATX in China).

2. Data sovereignty and sovereign clouds
In parallel with the technological proliferation in electronics for data storage and processing (3D NAND, neuromorphic chips, quantum computing, photonic computing, integrated photonics, photonic interconnection networks, high-performance computing (HPC), etc.), the number and volume of databases is growing exponentially (big data). The issue of securing these data sets is becoming increasingly important, whether for sovereign reasons (public services, critical databases), economic reasons (protection of sensitive company data), or for citizen reasons (citizen's rights, protection of personal data, right to be forgotten, etc.).

Launched in May 2021, the national " Trusted Cloud " strategy has had the merit of laying the foundations of a legal framework aimed at ensuring that French government data cannot be hosted directly by companies that are not under the exclusive control of French jurisdictions. This strategy is built around three pillars:

a/ The "Trustworthy Cloud" label, issued in accordance with the standards of the Agence nationale de sécurité des systèmes d'information (ANSSI).

b/ The "Cloud in the center" policy for the public sector (based on the SecNumCloud standard).

c/ An industrial policy implemented as an extension of France Relance.

In this regard, NumSpot, a collaboration between Docaposte, Banque des Territoires, Dassault Systèmes and Bouygues Telecom, aims to establish an independent, sovereign cloud offering in France. This initiative uses Dassault Systèmes' OUTSCALE cloud infrastructure, qualified as SecNumCloud, to offer services that meet performance, security and environmental responsibility standards. Since its launch in autumn 2022, NumSpot has trained a team of one hundred experts and established partnerships with major cloud players.

The French sovereign cloud ecosystem expanded significantly in 2025. At the end of 2025, the PREMI3NS offering from S3NS – 95% owned by Thales and 5% by Google, and operating on Google Cloud Platform technology – obtained SecNumCloud qualification, illustrating the possibility of combining hyperscaler performance with a sovereign trust framework. Other players are currently undergoing qualification, including Bleu, Scaleway and OVHcloud. In terms of adoption, the government's "Cloud at the centre" doctrine, which requires the use of cloud for any new government digital project, generated €84m in orders in 2025, up 62% compared with 2024, of which 70% went to European providers. This confirms the acceleration and increasing maturity of the French sovereign cloud ecosystem.
The SecNumCloud market remains modest at national level, estimated at €18m, but its European potential is estimated at €600m, highlighting the long-term industrial importance of this sector.

3. Digital identities
Closely linked to data sovereignty, the redefinition of digital identities also stems from digital transformation and the widespread adoption of remote procedures. The current landscape in France remains characterised by the coexistence of multiple digital identities with heterogeneous levels of security: strong identities, such as SIM cards, bank cards and passports; substantial identities, such as La Poste's Digital Identity; and weak identities, often issued by non-European players such as GAFAM. This fragmentation raises issues relating to personal data protection and technological control.

The alternative promoted by European authorities is based on the deployment of a strong, certified, unique and sovereign digital identity associated with the user, from which secondary identities could be derived according to different use cases.

The French industrial sector has the skills required to support this ambition, including secure elements, IAM, integration, cryptography, biometrics and PVID. Initiatives in this direction are multiplying in France, around the Electronic National Identity Card and FranceConnect, and at European level, through the eIDAS2 regulation and the European Digital Identity Wallet.

The European Digital Identity Wallet represents a major step forward in the standardisation and security of digital identity within the European Union. Tested as part of the POTENTIAL project, led by the French Ministry of the Interior and bringing together 20 countries, this digital wallet aims to enable every European citizen to access public and private services through a certified and interoperable identity. The use cases tested include access to public services, banking and telecom services, electronic prescriptions, driving licences and electronic signatures. Common technical components for issuing and verifying attestations are being deployed, particularly in a shared environment hosted by ANTS and open to the ecosystem.
Two new European projects have taken over since September 2025: APTITUDE, coordinated by Agence France Titres and bringing together 117 partners from 11 European countries, which is testing use cases related to travel and payment, including digital travel documents, vehicle registration documents and strong authentication; and WEBUILD, focused on use cases relating to legal entities, notably the management of corporate identity attestations and interoperability with national registers in a simplified KYC logic.

Beyond its technological dimension, the *Digital Wallet* also raises issues of adoption, trust and digital inclusion. Its widespread deployment will require public awareness-raising, the creation of integrated service ecosystems and compliance with European standards, particularly for age verification services, as provided for by the French law of May 2024.For example, several French players, such as Docaposte, have actively participated in these initiatives, notably through the POTENTIAL project, by developing components for issuing and verifying attestations and contributing to educational efforts around digital identity and the European wallet.
In parallel, in France, Docaposte is developing concrete identity verification and age-proof solutions linked to French regulatory requirements, notably through the 18Connect platform.

Passwordless authentication — passkeys and the FIDO2 standard. Password security has for decades been the weak link in the Digital Trust chain. The FIDO2 standard, developed by the FIDO Alliance with the support of Apple, Google and Microsoft, marks a technological break by offering authentication based on asymmetric cryptography and the hardware capabilities of devices, such as biometrics, embedded security modules or external hardware keys. In practical terms, during enrolment, the device generates a pair of cryptographic keys: the public key is transmitted to the service, while the private key never leaves the user's device. This results in authentication that is resistant to phishing, server compromise and replay attacks, whereas passwords and even SMS one-time passwords remain vulnerable. Passkeys are seeing accelerated adoption in 2025–2026, supported by native support in the main operating systems and browsers. From a regulatory perspective, FIDO2 is recognised as an authentication method that meets the requirements of the GDPR, NIS2 and PSD2. The European Commission's roadmap plans to complete the migration of critical use cases to phishing-resistant mechanisms by 2030. French and European players such as Thales participate in this ecosystem through their identity management and strong authentication solutions.

4. Digital transformation in particular is driving most cybersecurity segments: securing corporate clouds, telecommuting, intelligence and information gathering software that benefits from large digitally generated databases, etc.

FOCUS RESEARCH: PROGRAM AGENCIES AND CYBERSECURITY

In December 2023, the President of the Republic established seven "program agencies" within the French public research sector, with the aim of coordinating national research around major strategic priorities, particularly within the framework of France 2030. These program agencies aim to reduce the fragmentation of the French research system and improve the government's ability to direct scientific efforts toward economic, environmental, or technological issues it deems critical. The agencies thus represent a new mission entrusted to national research organizations.

To foster cooperation among organizations, universities, laboratories, and economic actors, the agencies seek to further orient public research toward major economic, health, environmental, and technological challenges. They must therefore become an instrument for the strategic steering of French research. Additionally:

• **they identify national scientific and technological priorities** in each of the major areas of their programs (foresight initiatives);

• **they design research and technology transfer initiatives** (technology, knowledge) based on these priorities and seek to secure state funding for them;

• **they manage these programs once they are launched;**

• **they bring together the academic community** (universities, schools, ONR) around these programs, thereby improving coordination among stakeholders in the French scientific system;

• **they also play a role in promoting French initiatives** in Europe and, more generally, internationally.

For example, in 2025, several new research initiatives were designed by the aforementioned agencies and funded by the government: Camelia focusing on AI components (shared by both agencies), Phoenix on component design and the Packaging initiative (ASIC agency), AI evaluation, Engineering Digital Twins, and AI for Scientists publication knowledge (Digital Agency).

Among the seven agencies created, two focus specifically on the field of cybersecurity, each with a dedicated program:

• **ASIC Agency for Digital Components, Systems, and Infrastructures** operated by the CEA, covering in particular hardware evaluation and all applications related to components, infrastructures, firmware, and embedded software; technologies for design, programming, evaluation, detection, and response to attacks; as well as infrastructure security

• **Digital Agency — Algorithms, Software, and Applications,** operated by Inria, which includes a cybersecurity program aimed at producing research results and innovation across the entire spectrum of software cybersecurity and at fostering and supporting the transfer of technology, skills, and knowledge from academic research to real-world applications and industry.

"Attacks today target the entire 'stack,' from applications to hardware components (including software-based attacks, such as Spectre), all the way down to the lower layers of the operating system"

In the field of cybersecurity, a research program (PEPR, currently falling under the two programs mentioned above and co-led with the CNRS) was launched in 2022 and will conclude in 2029. The time has thus come to reflect on and reassess the challenges and priorities that may lead, where appropriate, to continuing certain projects or supporting new ones.

This reflection takes many forms, but we can highlight here the work carried out by the agencies' various programs, in accordance with their forward-looking mission, based on the "National Strategic Review" published in July 2025 and within a framework established by the State.

In terms of cybersecurity, the digital transformation of critical infrastructure collectively exposes us to threats that are no longer limited to the exploitation of software vulnerabilities. Attacks today target the entire "stack," from applications to hardware components (including software attacks such as Spectre), through the lower layers of the operating system.

Given this reality, limiting security solutions to hardware or software is certainly counterproductive: an IT system based on a secure operating system deployed on a compromised hardware platform, just like an IT system based on a secure hardware platform but run by a vulnerable operating system, would remain exposed to attacks.

An integrated software/hardware approach therefore seems necessary to us. This is why the agencies' cybersecurity programs have proposed building a comprehensive and verifiable IT environment, from hardware microarchitecture to the user space, focusing on :

• **hardware security assessment:** identifying, measuring, and documenting attack surfaces present in hardware components (processors, microcontrollers, memory, communication interfaces, etc.);

• **the development of an OS with security properties that are formally defined,** verifiable, and anchored from boot time in the guarantees offered by the underlying evaluated hardware.

This project aims to generate a momentum that can ultimately only be European, to reduce dependence on opaque proprietary solutions and thus regain our digital sovereignty, while increasing our resilience.

2• Innovations specific to the sector that generate new products

At the same time - and given that digital trust is made up entirely of electronic and digital solutions - **innovations from digital trust** itself generate new products, **new applications** and thus growth.

1. Cryptography

Cryptography covers all processes designed, for example, to encrypt information in order to ensure confidentiality between the sender and the recipient. Technological developments in cryptography are numerous, and both French industry and the French training and research ecosystem are among the best in the world in this field. In addition to technological areas that are already relatively mature, such as public-key cryptography, the main areas of innovation are as follows.

• Lightweight cryptography.
The rapid development of IoT has a major impact on all aspects of cybersecurity. Recent large-scale attacks on IoT configurations have shown that robust cryptographic techniques must be used to ensure overall system security. However, in the case of IoT, where cost is an important parameter, the use of cryptography can be limited by the size, power and local computing performance of objects. This has given rise to a very active field of research around so-called lightweight cryptography.
In short, lightweight cryptography seeks to develop new cryptographic algorithms or protocols suitable for implementation in constrained environments, including RFID tags, sensors and healthcare devices. Lightweight cryptography will gradually be used in all IoT domains where the SWAP concept – size, weight and power – becomes critical.
The first industrial applications are currently being developed and

• Post-quantum cryptography.
cryptography. Communications, whether terrestrial or satellite-based, play a central role in society, and effective tools have been developed over recent decades to secure exchanged data and protect against attacks. However, quantum computers and their potential computing power represent a threat to data encrypted using current methods, as they could decrypt it in record time. To address this threat, post-quantum cryptography relies on new mathematical concepts to encrypt messages and secure the transmission of information. It is in this context that several projects have emerged, including the RESQUE consortium, which brings together sixcFrench entities – Thales, TheGreenBow, CryptoExperts, CryptoNext Security, ANSSI and Inria, together with six affiliated academic institutions – in a three-year project to develop a post-quantum cryptography solution. The project aims to secure communications and infrastructure against potential attacks from quantum computers. Funded by the French government and the EU, with additional support from Bpifrance, it focuses on the creation of a hybrid post-quantum VPN and a high-performance post-quantum HSM. These projects also extend beyond France, as illustrated by the partnership between Thales and the leading Korean mobile operator SK Telecom to develop post-quantum cryptography for 5G networks.

The French dynamic in post-quantum cryptography is accelerating under regulatory and institutional impetus. ANSSI has announced that, from 2027 onwards, it will no longer accept for qualification security products that do not integrate postquantum cryptography, and that after 2030 it will no longer be reasonable to acquire products without post-quantum cryptography. These milestones form part of a common European roadmap, adopted by Member States in June 2025, which sets the start of the transition by the end of 2026 and the protection of critical infrastructure by the end of 2030 at the latest. In terms of first concrete achievements, in October 2025 ANSSI issued its first two security approvals for solutions integrating post-quantum cryptography algorithms: Thales' MultiApp 5.2 Premium smart card and Samsung's S3SSE2A microcontroller, both using the ML-DSA signature scheme and evaluated by CEA-Leti, the first centre accredited for the post-quantum cryptography scope. These first certifications confirm the availability on the French market of trusted products integrating post-quantum cryptography.!
At the same time, the ecosystem of evaluation centres is being strengthened. Almond's CESTI laboratory, operated by Amossys, is in the process of being accredited for this scope, alongside Quarkslab, Synacktiv and Thales/CNES.

Beyond product evaluation, players such as Almond are already supporting software publishers and organisations in their transition to post-quantum cryptography. This activity includes inventories of cryptographic assets, audits of existing algorithms, the definition of migration plans and the implementation of hybrid architectures

Homomorphic encryption.
The rise of cloud computing has generated a highly active research field around functional encryption and homomorphic encryption. Functional encryption is a new paradigm of public-key encryption that enables both fine-grained access control and selective computation on encrypted data. In its most advanced form, fully homomorphic encryption allows computations to be performed on encrypted data without ever decrypting it: one party can encrypt data, another party – without having access to the key – can process it, and only the key holder can then access the decrypted result. This field is highly promising, and the first industrial applications are emerging. Iliadata is part of this dynamic. By combining secure multiparty computation and homomorphic encryption technologies, it offers solutions for confidential data pooling, enabling several stakeholders to collectively use data without compromising its confidentiality. This innovation was awarded the Research Prize at the 2025 Forum InCyber, underlining the growing relevance of these technologies inapplications are emerging. Iliadata is part of this dynamic.
By combining secure multiparty computation and homomorphic encryption technologies, it offers solutions for confidential data pooling, enabling several stakeholders to collectively use data without compromising its confidentiality. This innovation was awarded the Research Prize at the 2025 Forum InCyber, underlining the growing relevance of these technologies in

DNA-based cryptography.
This is a new branch of cryptography. It uses DNA as a vector for information and computation through molecular techniques. It is a relatively new field that emerged following discoveries regarding the very high storage capacity of DNA, which is the basic computing tool in this field. One gram of DNA can store around 108 TB of data, exceeding the storage capacity of any electrical, optical or magnetic storage medium. The first industrial applications are expected to emerge in the coming years.

Cryptography uses generative adversarial networks.
Generative adversarial networks are a recent innovation in artificial intelligence. The use of these algorithms in cryptography can improve the quality of certain systems. This field remains at the development stage for now, and the first industrial applications are expected to emerge in the coming years.

2. Secure elements.

This innovative field is particularly important for France, as all the underlying technologies originated there, enabling the development of three world leaders from France: Thales, IDEMIA and STMicroelectronics. Secure elements are micro- or nanoelectronic components combining secure embedded software and hardware, designed to be integrated into communicating devices in order to securely manage all interactions between these devices and the outside world, by storing dedicated applications and confidential data in encrypted form, such as SIM cards and bank card chips.

In the context of IoT development, the secure elements segment is marked by the replacement of SIM cards, or Universal Integrated Circuit Cards, by miniaturised secure elements that are directly embedded or integrated into the systems to which they belong, or even by solutions with no hardware component, such as soft secure elements and Trusted Execution Environments.
The deployment of embedded secure elements, or e-UICC, and soft secure elements is now well advanced. The e-UICC has become widely established in smartphones, wearables, laptops and the automotive sector, driven by the massive adoption of eSIM.

The next frontier is iSIM, or integrated SIM / i-UICC, which integrates SIM functionality directly into the device chipset, thereby removing the need for any separate component The first iSIM architectures are in early deployment, notably in high-end smartphones and automotive applications, with joint Qualcomm-Thales validation on Snapdragon 8 Gen 3. However, mass deployment is still to come. At the same time, the new GSMA SGP.32 standard, which aims to unify M2M and consumer approaches for IoT, is in the early stages of deployment in 2026 and should accelerate eSIM adoption in industrial fleets and constrained environments.

Thales and IDEMIA remain among the world leaders in this ecosystem, alongside Giesecke+Devrient and STMicroelectronics. There is a potential medium-term threat for French players due to the lack of expertise in Europe and France in More technologies, which could lead US and Asian manufacturers to acquire dominant positions in the i-UICC segment. Soft secure elements also represent a significant threat for French players, mainly through US GAFAM and Chinese BATX players, which can leverage their dominant positions to impose their own solutions.

Application security and cyber certification — Security by Design.
The multiplication of cyberattacks exploiting softwarevvulnerabilities, combined with growing European regulatory requirements – foremost among them the Cyber Resilience Act, which imposes security-by-design requirements for all digital products placed on the EU market – gives growing strategic importance to securing applications and software from the development phase onwards. This principle, which consists of integrating security requirements from the design stage of a product rather than adding them afterwards, is becoming both an industrial and regulatory imperative.

Product certification is the cornerstone of this dynamic. In France, the certification system is structured around several schemes supervised by ANSSI: First-Level Security Certification, or CSPN; Common Criteria for in-depth evaluations; and now the new European EUCC scheme, the Common Criteria-based European Cybersecurity Certification Scheme, adopted by the European Commission in January 2024 under the Cybersecurity Act. The EUCC is intended to gradually replace national schemes and become the unified cybersecurity certification standard at EU level, enabling a certificate issued in France to be recognised across all Member States.

France is particularly well positioned to benefit from this European certification dynamic. In October 2024, Almond launched its Security Evaluation & Analysis Lab, or SEAL, a technical cybersecurity laboratory bringing together the analytical capabilities of its expertise division and those of the CESTI operated by Amossys, which has been accredited by ANSSI since 2011. In October 2025, SEAL obtained EUCC approval at the Substantial and High levels, making Almond one of only two French laboratories authorised to evaluate and certify software and network equipment according to the strictest standards: CSPN, Common Criteria and EUCC. Beyond certification, SEAL conducts advanced offensive analyses, supports software publishers in adopting a Security by Design approach from the development phase, and contributes to the transition towards post-quantum cryptography. Its stated ambition is to become a laboratory with a European dimension, also accessible to SMEs and software start-ups, in a context where European regulatory obligations are creating strong structural demand for certification expertise.

3. Artificial Intelligence (AI).

Artificial intelligence covers the development of machine learning algorithms, including artificial neural networks, whether multilayer or not, supervised or unsupervised, and generative adversarial networks, for prediction or classification purposes. It also includes generative text AI, such as ChatGPT, and edge AI, meaning the design of chips and embedded systems dedicated to running machine learning algorithms, which require very high computing and memory capacity. Developments in artificial intelligence are not specific to the security sector, but they do require the establishment of a framework for trusted AI.

• **The need for a legal framework:** the development and use of AI must be aligned with society's fundamental values. This requires European legislative work to establish a stable legal framework that protects citizens' rights and freedoms while enabling technological innovation. This framework must take into account several aspects of AI, including its technical nature and liability, and must be developed in a coordinated way in order to form a coherent and robust foundation. The challenge is to regulate AI by eliminating potential risks without preventing innovation, so as not to deprive society of essential tools for its digital sovereignty and strategic autonomy.

• **A definition of trustworthy AI:** AI systems must be designed to be transparent, explainable and secure. Trust in these systems can be strengthened through strict cybersecurity standards and rigorous development processes designed to anticipate potential vulnerabilities and abuses. In addition, the data used during the training phase of these AI models must be managed ethically, with clear standards to prevent the introduction of discriminatory bias, in order to ensure that the decisions made by these models are fair and equitable.

• **Social acceptance of AI:** Social acceptance is essential and must be cultivated through an ethical approach to deployment. Respecting ethical principles, protecting human rights and prioritising human well-being in the development of AI are fundamental. Public education and awarenessraising, combined with transparent demonstrations of the usefulness and safety of AI, for example during major events, can help improve understanding and acceptance of these technologies.

ACN White Paper: "Blockchain"

available at the following link:
www.confiance-numerique.fr/publications/

In artificial intelligence, France benefits from excellence in training and research, and French security players are taking strong positions in security applications, notably Thales Digital Identity & Security and IDEMIA. Although France lags behind the United States and China, which are leveraging their powerful digital industrial bases, it has a competent industry in industrial AI and generative AI. However, France is also experiencing a brain drain to the United States in this field, which threatens French positions in the future, including in the security sector.

4. Blockchain

Initially associated with crypto-currencies and Bitcoin in particular, blockchain is emerging as a new essential tool for digital trust. This protocol records and stores transactions in encrypted form in a decentralized database. The information is, in fact, unforgeable and unchangeable. As a distributed and secure register of transactions, the blockchain is both a vector of trust and a tool to fight against fraud. It is either public (all participants can intervene in the process) or private. In the latter case, only certain participants record transactions and authorize or not their reading. There are many developments in the field of digital trust: management of social benefits, protection of the infrastructures of vital operators, but also civil or internal security missions and secrecy management between institutions.

These applications will reduce dependence on a central authority, but they require the evolution of the current centralized trust system towards a decentralized system for sovereign-type applications as well as a new organisation of operations. French players have mastered several of the key technologies in the field of blockchain (cryptography, formal methods, etc.).
However, it should be noted that the level of acceptance of the technology by users is still low. At the global level, all sectors taken together - and although this technological field is still not very mature - the American industrial ecosystem is clearly the most advanced in the development of solutions integrating blockchain. The Chinese ecosystem is also important and growing rapidly. Finally, the German and British ecosystems are at least comparable to the French ecosystem.

Open Hardware/Software platforms for edge computing and IoTs.
Sharing software code (Open Software) has been around for some time, but in recent years the trend has been towards sharing electronic component designs (Open Hardware). Open source software and hardware accelerate innovation by allowing developers and designers to share and reuse developments made by others.

The re-publication of new developments in open source fuels the innovation process and benefits the whole community. France's strengths in this area of Open Source are numerous. The national market is highly developed, representing a quarter of the European market.

The community of both researchers and developers is undoubtedly the largest and most advanced. However, security is not very present in the Open Source world. The security
market is still dominated by the major proprietary software publishers, most of them North American. A proactive purchasing policy and incentives for the development of certified technology bricks and platforms oriented towards Open Source would help to strengthen this field, particularly for innovative applications associated with edge computing or IoTs, where American domination is not yet too strong.

6. Real-time analysis of local and wide area observation data.
In terms of local observation and surveillance, real-time analysis will eventually be the keystone of the future video surveillance ecosystem. Coupled with artificial intelligence, it will make it possible to identify wanted individuals in real time or to make certain decisions automatically. Real-time satellite imagery is also developing, with numerous opportunities for wide-area observation and intelligence and information gathering. France has the players and the technological know-how to benefit fully from these technological developments.

7. Open Source Intelligence (OSINT).
OSINT has existed for decades in rudimentary form (human sources, documentation, bibliography, etc.).

It was with the explosion in the amount of open data available online since the early 2010s that the OSINT market really took off, through the development of IT tools for collecting and exploiting this data.

These data come from avariety of sources: social networks, websites, media, geospatial imagery, forums, measuring devices, etc., all of which represent a goldmine of information that can be exploited for intelligence purposes. Until the early 2010s, users of OSINT services were limited to government agencies for intelligence purposes or to combat fraud, crime and misdemeanors, as well as a few large corporations, notably through business intelligence agencies.

Today, we can see the emergence of an ecosystem of companies capable of providing OSINT solutions, the most important of which are Chapsvision (notably with the acquisition of Owlint), Palantir, Thales, Athea, Airbus (GEOINT), Anozr Way, Sekoia.io, etc.

8. Zero Trust architecture.
Faced with the widespread adoption of hybrid cloud, remote working and the fragmentation of traditional security perimeters, the Zero Trust model has become the reference paradigm for security architecture. Its founding principle – "never trust, always verify" – requires continuous authentication of every user, device and flow, regardless of whether they are located inside or outside the network.
This model is now closely linked to regulatory compliance. The European NIS2 Directive, transposed into French law and applicable to more than 15,000 French entities in critical sectors such as energy, transport, healthcare and digital services, is de facto pushing organisations to adopt Zero Trust architectures in order to meet its requirements for risk management, access control and continuous monitoring. The French ecosystem includes players that are well positioned in this sovereign market, with solutions certified by ANSSI: Stormshield for network segmentation, Wallix for privileged access management, and Sekoia.io and HarfangLab for threat detection and response. In 2025, ANSSI published a guide dedicated to the implementation of Zero Trust in public administrations, making this architecture an institutional recommendation.

9. Other technological developments also exist, but they do not have the same level of impact on the global Digital Trust sector. Developments around digital identity provide one illustrative example, **including CAPTCHAs and software challenges, QR codes, iris recognition, vein pattern recognition and dynamic passwords.**

3• Digital transformation & miniaturization: Towards global offers of Security as a Service

1. The security sector as a whole is in the process of standardizing its products

At the global level, digital trust is impacted by two major factors:

• **Miniaturization coupled with the falling cost of electronic components**, leading to an ever-increasing share of electronic systems or sub-systems in security products.

• **Digital transformation**, leading to an ever-increasing share of software in security tools. In particular, producers of physical and electronic products - where margins are on average lower than in cybersecurity - are progressively trying to move up the value chain by developing skills in software. The latter - such as Thales, Idemia and Naval Group - are positioning themselves more and more strongly in the development of software dedicated to application security.

The intersection of the two trends described above is therefore gradually leading the players in the industrial sector to position themselves in all segments: physical, electronic and cyber. The physical/electronic/cyber distinction is consequently progressively going to have less and less meaning and in the long term it is likely that each product architecture will be global with a physical component, an electronic component and a cyber component.

This trend even affects private security services. Whereas the physical security of premises used to be made up solely of human resources, its technological and electronic content is continually increasing (SOC, video surveillance cameras, etc.), thanks to the miniaturisation and falling costs of electronic products.
In human surveillance, net profitability is very low (only 1% on average in 2021 and artificially boosted by the CICE). In electronic security, it is higher, although with varying levels depending on the company.
The desire of a large number of private service providers is therefore to diversify their services by integrating electronic and cyber products and by moving upmarket.

For example, the large Spanish company Prosegur, one of the European leaders in security, has created an investment fund with €30 million to invest in electronic and cyber security. Since 2016, this fund has acquired the companies Dognaedis, Innevis and Cipher, all of which specialise in cyber security and are grouped together within Prosegur under the Cipher brand.

Securitas, another European leader in private security, acquired the electronic security business of the American Stanley Security in January 2022 and is expanding in this segment.

Finally, this trend is also felt by the buyers in the industry. All players concerned by security issues (and OIVs in particular) must now also integrate cyber security as a strategic issue.

Suez is an emblematic example of a player traditionally concerned with security through the management of drinking water networks and which now considers cybersecurity to be a strategic issue. Calls for tender for the digitalisation of drinking water management increasingly include cyber-security aspects of the data generated.

2. This standardisation is leading manufacturers to develop more and more global turnkey offers...

Global turnkey cybersecurity offer, global Safe City offer, global security offer, etc. more and more players in the sector are positioning themselves on this type of global offer by following the product standardisation dynamic mentioned above.
Thales, through the acquisition of Gemalto in 2019 and the creation of the «Digital Identity & Security» Business Unit bringing together Gemalto, the Thales Digital Factory, Guavus (an American specialist in Big data analytics acquired in 2017) and Thales eSecurity (following the acquisition of Vormetric in 2015), is the most emblematic example of this type of strategy, with the aim of providing and securing the entire critical decision chain in a digital environment. Atos, Orange, Equans and IBM are also positioned on global offers.

3. ...open source...

Some players offer turnkey approaches with proprietary systems. These approaches are less and less favoured by customers who find themselves dependent on a single private player for the maintenance and future improvement of interfaces. As a result, the development of open source solutions is increasing.

In the particular field of national identity management systems (civil status) operated by states, the trend towards the use of open source solutions is also noticeable.

However, there is also a very strong trend towards modularity in terms of distinct functional bricks, as States wish to avoid being dependent on a single supplier or service provider so as not to be locked in. This is reflected in particular in the use of standardized APIs (Application Programming Interfaces) for each functional brick, ensuring complete independence in their design, while allowing them to be interconnected in an interoperable manner.

This trend is combined with that of open source, as functional bricks are increasingly based on open source solutions. This issue of API standardisation is gaining momentum on many subjects, for example with the concept of Open-Services Cloud (OSC) aiming to make cloud services interoperable, reducing the dependence of cloud users on hyperscalers (see the DECISION Études & Conseil study carried out at the beginning of 2023 on the subject: *Open-Services Cloud (OSC) Unlock Cloud interoperability to foster the EU digital market*.

4. ... And As a Service

At the same time, we are seeing the gradual end of the simple purchase of products (software in licence mode, etc.), and the development of sales in the form of services (SaaS: Software as a Service, etc.), guided by the need for constant adaptation of security tools to deal with new threats in a context of constant technological change.

In 2020, the provision of software in SaaS mode already represented 40% of the total value of the European enterprise software market (DECISION Études & Conseil, SITSI).
This proportion is growing year on year and should approach 80% by 2030.

As far as solution providers are concerned, this change in usage does not offer new markets or opportunities. On the other hand, it is changing the way companies design their solutions.

As a result, it offers an opportunity to reshuffle the deck in all markets, as current leaders who fail to reshape their solutions and the business models based on these solutions will lose their leadership positions in the coming years.

On the customer side, security is gradually becoming an organizational skill that is found in all the people involved in the design of products and services, and no longer just a separate function isolated from the application development process or associated skills.

One of the consequences is the progressive development of dedicated internal teams in each of the clients' operational units.

ACN

Alliance pour la confiance numérique

The Alliance pour la Confiance Numérique (ACN) represents companies in the Digital Trust sector, including world-leading companies, SMEs, micro-enterprises and intermediate-sized enterprises, particularly in digital identity, cybersecurity and trusted AI.

France has a highly competitive industrial base in this field and internationally recognised excellence, supported by global leaders, SMEs, intermediate-sized enterprises and a wide range of dynamic players across the sector.

The sector comprises 2,572 companies, generating €22.4bn in revenue in France, in a fast-growing market that has recorded average annual growth of 7% since 2016.

The 95 members of the Alliance pour la Confiance Numérique (ACN), 80% of which are SMEs, micro-enterprises or intermediate-sized enterprises, account for two thirds of the worldwide revenue generated by French Digital Trust companies. These members include hardware manufacturers, software publishers, integrators, service providers, security assessment laboratories, research organisations and others.

ACN is a member of the FIEEC – the French Federation of Electrical, Electronic and Communication Industries – an associate member of Campus Cyber, and actively contributes to the work of the Strategic Committee for the Security Industries.

ACN is also a founding member of ECSO, the European Cyber Security Organisation, which represents the European cybersecurity ecosystem.

ACN partners

ACN members

ABOUT
DECISION ETUDES & CONSEIL

Since 2017, DECISION has been conducting the Digital Trust Industry Observatory on behalf of ACN.

DECISION is a research and consulting firm specializing in economic studies (market analysis, forecasts, value chains, etc.) and consulting and strategy assignments, in the fields of:

- electronics (components, equipment, systems),
- aeronautics, defense, security,
- electricity, renewable energies and industry of the future.

Our customers include private companies, whether start-ups/SMEs/ETIs, major industrial groups, professional organizations or financial institutions and investment funds, as well as local and national public authorities (governments, ministries, etc.) and the European Commission.

In 2009, DECISION initiated and conducted the first study for the European Commission on the security industry, and is one of the partners in the framework contract (2010-2015) on the security industry (including cybersecurity) for the European Commission's DG ENTR.

Since then, DECISION has also carried out studies to assess the economic weight of the security industry for the French government:

- In 2015 under the aegis of PIPAME (Pôle Interministériel de Prospective et d'Anticipation des Mutations Economiques), an inter-ministerial structure bringing together the Ministry of the Economy (DGE), the Ministry of the Interior (DMISC) and the SGDSN.

- In 2018 under the aegis of CoFIS (Comité de la Filière Industrielle de Sécurité), bringing together the Ministry of the Economy (DGE), the Ministry of the Interior (DMISC), SGDSN, CICS (Conseil des Industries de la Confiance et de la Sécurité), GICAT and Milipol.

- In 2020, under the aegis of the Conseil Stratégique de Filière (CSF) des Industries de Sécurité, bringing together the Ministry of the Economy (DGE), the Ministry of the Interior (DMISC), SGDSN, CICS (Conseil des Industries de la Confiance et de la Sécurité), and GICAT.

- In 2022, through a consortium including GICAT, ACN, the Ministry of the Interior, the Ministry of the Economy (DGE) and SGDSN.

For more information
www.decision.eu

DECISION
ETUDES & CONSEIL

ACN

Alliance pour la confiance numérique

Inspire Unify Empower Act

English version available at :
www.confiance-numerique.fr