2024

Alliance for Digital Trust

confiance-numerique.fr

Observatory of Digital Trust Sector

ACN

Alliance pour la confiance numérique

SOMMAIRE

A WORD FROM ACN - ALLIANCE FOR DIGITAL TRUST

Daniel Le Coguic
ACN Chairman

Observatory for the digital trust sector, which ACN is honoured to present for the 10th consecutive year, provides an increasingly detailed analysis of the changes taking place in our industry. It makes a significant contribution to our understanding and ability to anticipate develoSMEsnts in the digital trust sector and to deduce the strategies to be implemented so that our digital identity, cybersecurity, and trusted artificial intelligence companies can contribute to our country's digital sovereignty and the preservation of our fundamental values.

In the year 2024, a clear strategic vision is more necessary than ever to meet the challenges we face. Geopolitical conflict is reaching heights we haven't seen for decades, and the digital world is becoming an increasingly unbridled battleground where malicious acts are multiplying, driven by different motivations and objectives that intermingle, somISEmes merge, and amplify each other.

Given the inescapable role of digital technology in all our activities, it is now imperative that we get away from the relative naivety that has characterised our digital develoSMEsnt. This naivety has led us to make massive use of tools, particularly those from outside Europe, whose level of trust has hardly been questioned. Yet the risks are numerous, ranging from the malfunctioning of our systems to the capture of our personal or strategic data, the destabilisation of our democratic sociISEes, the exposure of our citizens, particularly the most vulnerable, and the loss of our strategic autonomy because of our overdependence on technology in certain key digital areas.

Let's hope that this return of tensions will open our eyes: there is an urgent need to place digital trust at the heart of our society. This major paradigm shift is in fact already underway, and we are delighted that our governments, at both national and European level, have begun this change of direction with real determination. We now need to accelerate and amplify the initiatives that have already been launched, mainly in three directions. First, we need to make up for past mistakes, not only by significantly increasing the number of digital trust tools and the resilience of all the players in our sociISEes, but also by continuing the regulatory and standardisation efforts underway in Europe and France. Some welcome pieces of legislation (proposed creation of a European

digital identity portfolio - EUID, proposed AI Act, Resilience of Critical Entities - REC, of financial entities - DORA - and of Essential/Important Entities - NIS2) are currently being debated: their rapid implementation will substantially raise our level of protection. These regulatory frameworks will shape the playing field for digital trust, and it is imperative for ACN to play a proactive role in these debates to defend the interests of French industry, with the aim of designing and developing technologies that are compatible with public and individual freedoms, and acceptable to citizens.

Secondly, we need to consolidate our achievements and capitalise on a dynamic, high-performance digital trust industry. The year 2023 saw robust growth (9.6%) for our sector, with sales reaching €19 billion in France and €31 billion generated worldwide. Employment in the sector has also risen significantly, with 89,000 people now employed in France and 145,000 worldwide. These figures not only illustrate the vitality of our sector, but also underline the crucial importance of digital confidence in the economic and social fabric. Our companies, whether world leaders or innovative SMEs/start-ups, are making an active contribution to securing and structuring the new digital space, while fostering innovation and compISEtiveness. It is vital for this teeming ecosystem to find market outlets that will enable it to face up to international compISEtion under conditions comparable to those of compISEtors from other geographical areas. The notion of a domestic market is crucial in this respect, which is why the European Union must move as quickly as possible towards a single trusted digital market.

The rapid introduction of a «Buy European Trust Act», which ACN is promoting in its proposals for the 2024 European elections, would be a major step towards achieving this ambition.

Finally, preparing for the future is also a prerequisite if our sociISEes are to continue to live by the values that we all share, but which do not enjoy consensus in other parts of the world. This involves our research efforts and our ability to innovate constantly, so that we can master the technologies that are essential to our sovereignty. Trusted AI, post-quantum encryption and quantum computing are all subjects that intrinsically challenge our current model of society. Our country and our continent need to be at the cutting edge of innovation, whether in the technical, intellectual, or regulatory fields. We have considerable assets and world-renowned human and technical expertise : let’s not fall behind.

France is hosting the Olympic Games in Paris this summer, and the French digital trust industry and ACN have joined forces to make this major event a showcase for our expertise. «Higher, faster, stronger, together»: the Olympic messages resonate with our industry’s horizon.

In conclusion, 2024 must be a year of consolidation, action, and anticipation. We must continue to build on the successes of 2023 while adapting our approach to meet the challenges of tomorrow. As the standard-bearer for the digital trust industry, ACN’s mission is to ensure that, in this rapidly changing landscape, our sector plays its fundamental role in the service of national digital sovereignty and European strategic autonomy.
MeISEng these challenges will be a collective effort. All the players in the industry, from start-ups to major corporations, need to step up their collaboration, not only with each other but also with our public and private partners, to meet our common challenges: defending and promoting our fundamental values so that we can control our digital future and our future in general.

A WORD FROM THE MINISTER

Credit: Ministry of Economy, Finance and Industrial and Digital Sovereignty

Marina Ferrari
Secretary of state
for digital affairs

Against a backdrop of renewed geopolitical tensions, France and the European Union face major challenges in securing digital spaces in the face of the growing cyber threat, countering attempts to destabilise our democracies through massive disinformation campaigns, and better protecting the personal data of our fellow citizens. The digital transformation of our economy and our society is an inescapable reality that holds great promise. But it also brings with it a growing need for security, transparency, and reliability in the use of digital technologies, in a word, digital confidence. That's why this sector plays a vital role in supporting these changes. Digital identity, cybersecurity and trusted artificial intelligence are therefore at the heart of the Government's concerns, and my work as Secretary of State for the Digital Sector is based on two key priorities: resilience and sovereignty.

In terms of resilience, this year will resolutely see the implementation of concrete measures that will enable us collectively to better deal with cyber risk. The transposition of the ECR, DORA and NIS2 directives into French law is designed to raise the general level of digital security in France by enabling the much larger number of entities concerned to better protect themselves at every link in the value chain. To give these provisions their full force, it is essential to ensure that they are ambitious, but also proportionate, appropriate and reasonable for all stakeholders, especially the small and medium-sized enterprises that are at the heart of our digital economy. This is why the preparatory work on these texts was carried out in co-construction with the regulated entities to achieve a balanced implementation, thus promoting a robust digital environment, without hampering innovation or compISEtiveness.

The role of the digital trust industry is crucial in consolidating this framework. I know that I can count on the French ecosystem, which includes both major structuring players and many start-ups and SMEs that are technological nuggets. The challenge for the industry will be to ensure that the various service and technology providers work together effectively to develop integrated, coherent solutions that meet the needs of all users. As a trade association, the Alliance pour la Digital Trust (ACN) has a key role to play in stimulating collective action by companies in the industry.

This is also the reason for being of the «Je choisis la French Tech», which aims to encourage all public and private purchasers to better integrate the solutions available from our national pool of digital companies.

Strengthening our level of resilience, as well as our digital trust industry, is the sine qua non of our digital sovereignty, in an environment where both state and non-state actors exploit the IT vulnerabilities of our businesses and administrations to disrupt the smooth running of our society. Beyond the security issue, it is the defence of our democracy that is at stake.

To achieve this, we need to equip ourselves with the capabilities that will enable France and Europe to control, with the greatest possible degree of autonomy, the digital future of our fellow citizens. This means paying particular attention to training and awareness-raising, but also making a greater effort to develop and structure our ecosystem in strategic areas such as quantum technology and artificial intelligence. Trust, based on the triptych of legal, technical, and ethical criteria that ACN rightly sets out in its White Paper on Trusted Artificial Intelligence, must be our compass in building our digital future. The Government is strongly committed to this goal and is leading structural initiatives, notably through the France 2030 plan, to strengthen our economic fabric. The efforts we are making to support research and innovation, at both national and European level, should serve to create a leverage effect and ultimately strengthen our country's and Europe's skills in these areas.

Strengthening our digital sovereignty means ensuring that every citizen can identify and authenticate with the highest level of security when required, but also with the greatest ease of use. Under the impetus of the European Union, the creation of digital identity portfolios is firmly under way. These new tools will make it possible not only to secure exchanges but also to strengthen the protection of everyone's personal data and better protect minors from sensitive and shocking content. This too is a crucial issue for confidence in the digital world, and one to which the law aimed at securing and regulating the digital environment, adopted by Parliament on 10 April, provides ambitious solutions.

Protecting our fellow citizens, our businesses, our administrations, and our values in the digital space is more vital than ever. In the process, it is imperative that we retain our digital sovereignty as a guiding principle. In many respects, these are decisive times, and I am convinced that it is by working together that we will succeed in defending and promoting our values in the digital world. We have the means to do so.

KEY INSIGHTS

Digital Trust is crucial in our economy and in our society in the midst of digital transformation.

It includes **digital security** (digital identity, trusted electronic systems and subsystems), as well as cybersecurity (products/software and services).

The **Alliance pour la Digital Trust (ACN)** was set up to bring together and support the players in this sector in France and to ensure its institutional representation.

The ACN has set up the **Observatory of Digital Trust** to gather and study data on the main characteristics and trends of this sector. It is within this framework that this study was carried out in 2024, covering the field of cybersecurity and digital security.

Digital Trust in France in 2023 corresponds to :

€19 billion in revenue in France

- **€19 billion in revenue,** i.e. 9.6% growth between 2023 and 2022
- **€9 billion of added value**
- **89,000 people employed** in the sector
- **55% of revenue** from **cyber security** and **45% from digital security**

French Digital Trust companies in the world in 2023 represent :

€31.3 billion in international revenue

- **€31.3 billion in revenue** generated worldwide by the French Digital Trust industry (revenue in France, revenue exported from France and revenue generated abroad by companies owned by French shareholders)
- **World leaders** in digital security (Thales, Airbus D&S, Atos Eviden, ST Microelectronics), identity and access management (Thales, Idemia, IN Groupe, Docaposte), cybersecurity services (Thales, Atos Eviden, Orange Cyberdefense, Sopra Steria, Capgemini), and secure payments (Worldline)
- **€18 billion in international revenue,** i.e. 57% of total revenue (revenue exported from France and revenue generated abroad by companies owned by French capital)
- **€5.7 billion of revenue exported from France,** an average export rate of 30%.

Digital Trust is a thriving industry :

9.6% growth in France in 2022

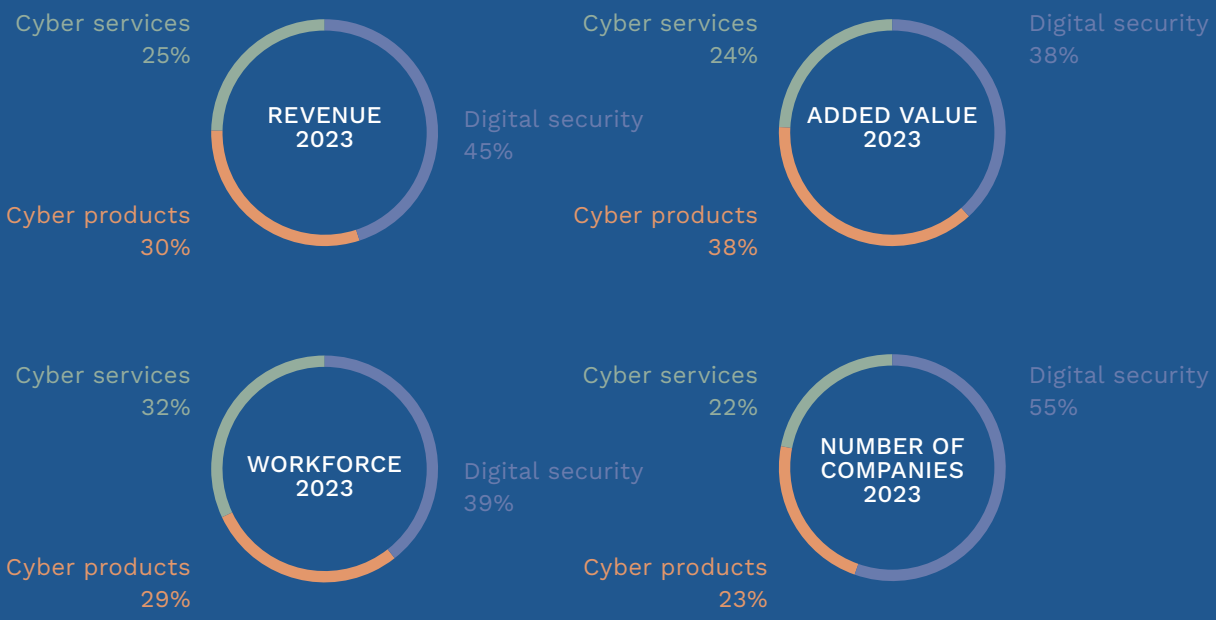
- **8%** average annual growth in France over the 2018-2023 period, compared to **0.7%** for the French GDP* (*GDP growth measured by INSEE in chained volume)
- Digital Trust is the **French industrial sector that has experienced the strongest growth over the past 10 years**
- **Digital Trust has shown itself to be particularly resilient in the face of the COVID crisis in 2020,** with 3.6% growth in 2020 compared to -7.8% for the French GDP
- Digital Trust is **the most productive sector,** i.e. with the highest ratio of added value to revenue

Digital Trust is an ecosystem of companies of all sizes :

2 178 companies in the sector in France

- **2,178 companies in the sector in France**
- Of which **75 are large entreprises**
- Of which **69 ISEs** (Intermediate-sized enterprises)
- Of which **635 SMEs** (Small and Medium-sized Enterprises)
- Of which **1,399 Micro-entreprises**, generating less than 2 million in revenue in 2023

Main sectors in Digital Trust



Sources : DECISION études et conseils

KEY FIGURES 2023

Revenue

€31.3 B of global revenue

- €12.3 B of revenue abroad
- €19 B of revenue France
  - Included 5,7€ B of exported revenue

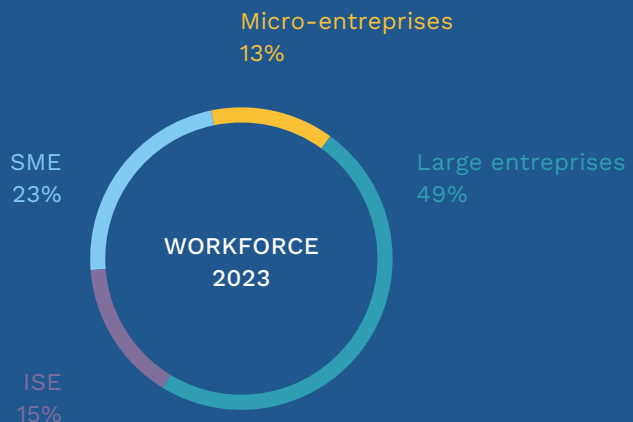
€9 B AV* France

*(added value)

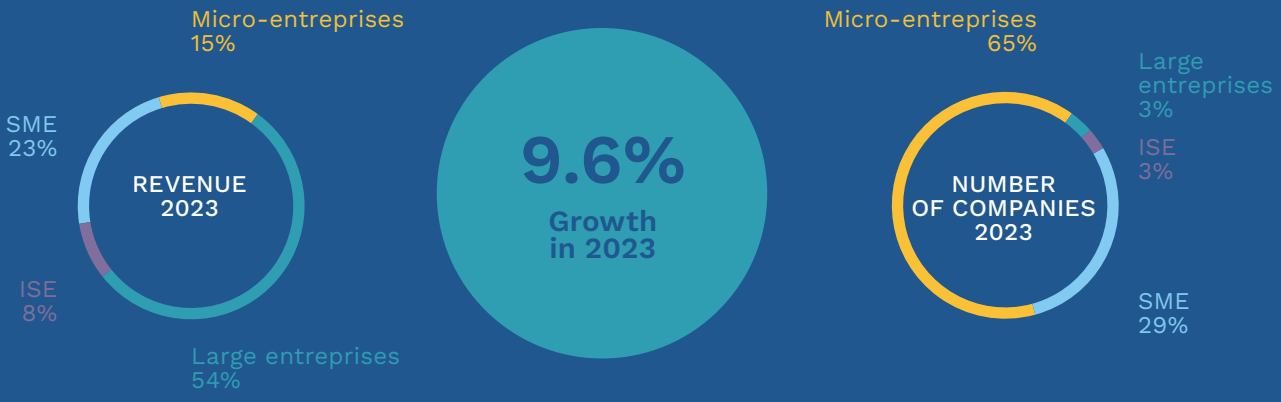
Workforce

89 000
Workforce in France in 2023

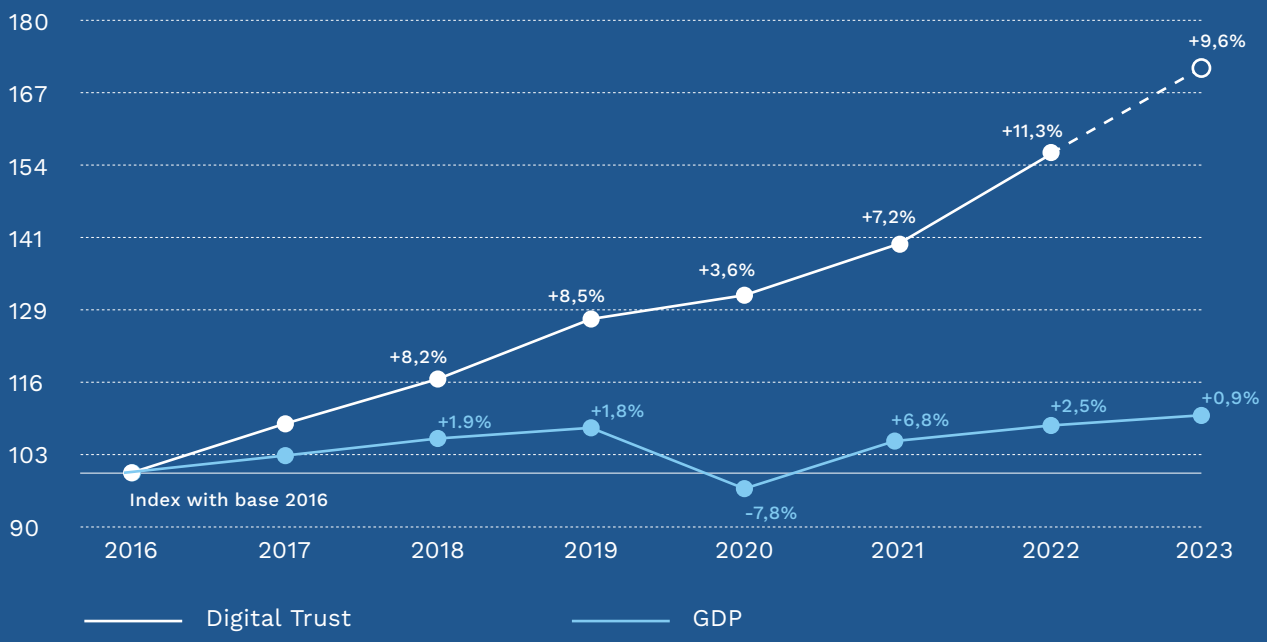
144 700
Workforce abroad in 2023



Growth



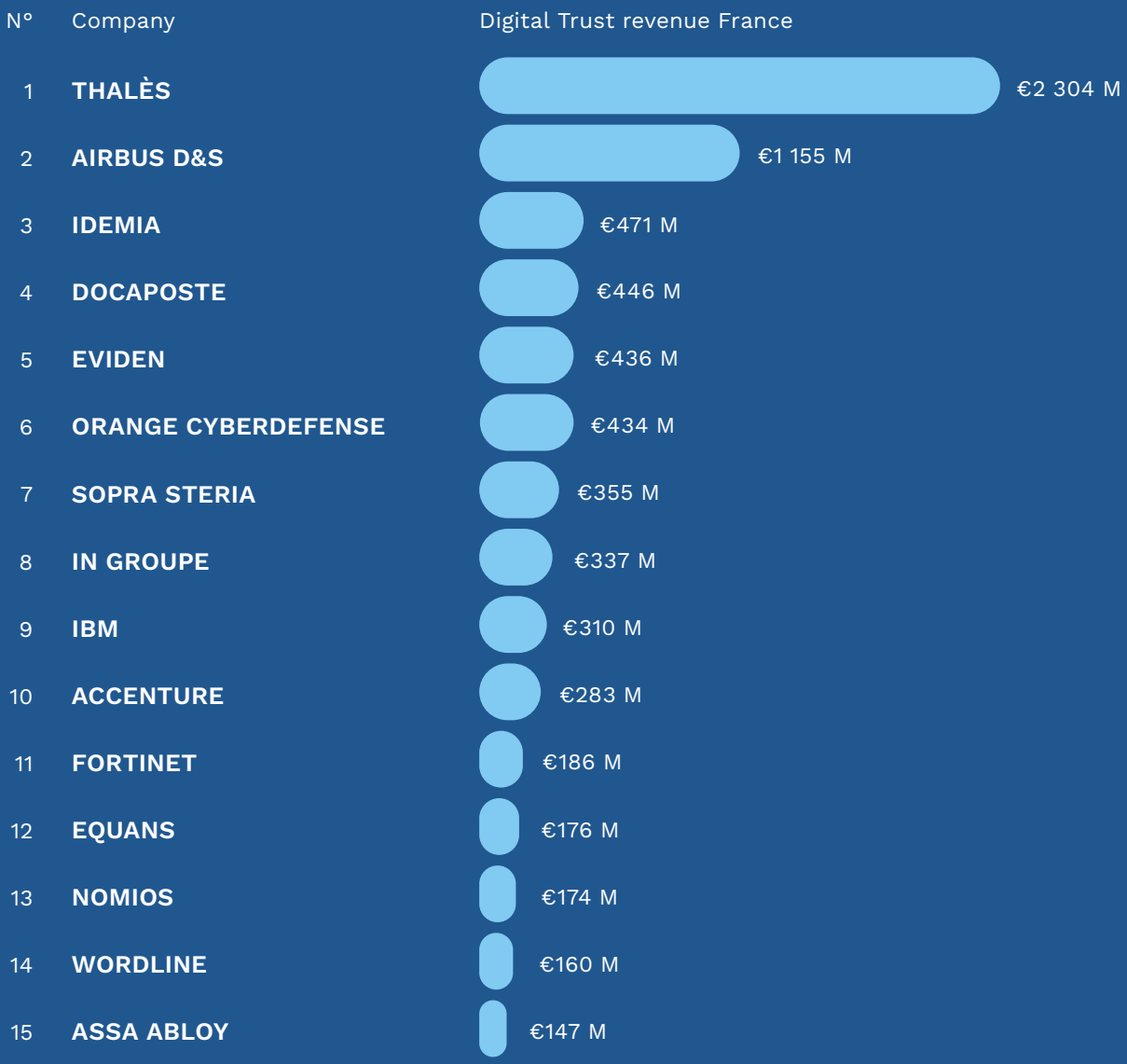
France growth comparison 2017-2023



GDP growth measured by the INSEE and IMF for 2023

Source : DECISION Etudes & Conseils

Top 15 players France



- Thales includes Gemalto 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, Owlint and Geotrend
- Idemia includes Otono networks
- IN Groupe includes Surys et Nexus
- Econocom includes Exaprobe
- Worldline includes Ingenico
- GFI Informatique includes SIS
- Cisco includes Sentryo
- Sogetrel includes Eryma

Emergence of an ecosystem of distributors of cybersecurity and services

Top 1-10 players in France

Top 10-20 players in France

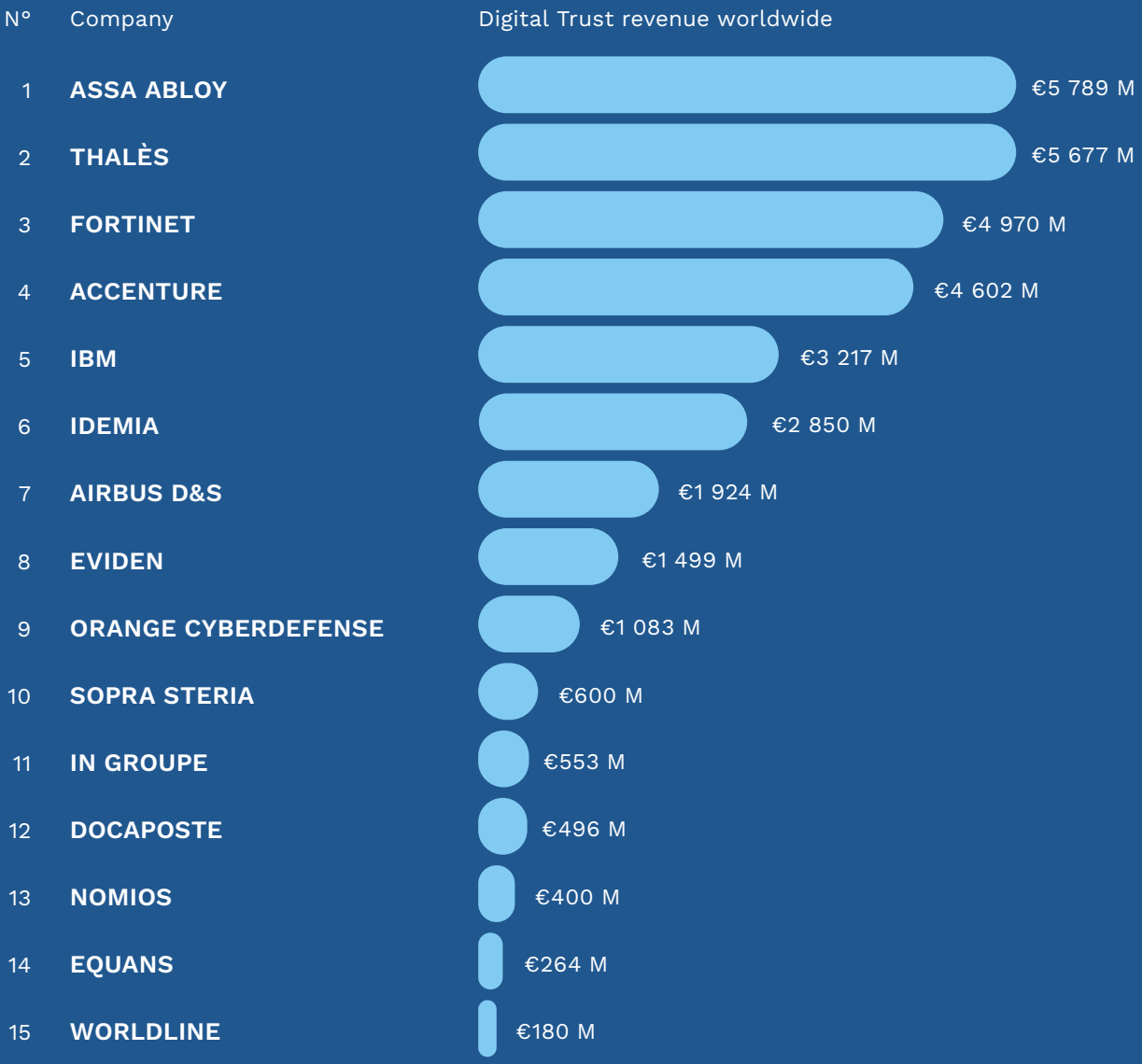
French Digital Trust revenu in between €115M & €230M

Top 20-50 players in France

French Digital Trust revenu in between €40M et €100M

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

Top 15 players worldwide - 2023



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

■ **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, 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.)

ACN IS AT THE CORE OF THE INDUSTRY

Among the ACN members there are :

■ **14 large entreprises or ISE, including the 9 French leaders in Digital Trust.**
■ But also more than **100 SMEs, VSEs and innovative startups as direct members** and more than **200 SMEs in the sector** via the ecosystems of its partner members (Bretagne Développement Innovation, Pôle SCS, SPAC, etc).

ACN members account for :

I. DIGITAL TRUST : CYBERSECURITY AND DIGITAL SECURITY

Among the players ranked between 10th and 20th and with a revenue of more than €115 M from France in 2023, there are French players such as Cap Gemini and Nomios (cyber services), Worldline (payment security), Safran, Equans (digital security) and Selp (identification and secure documents) as well as foreign players such as: Assa Abloy (Access control and authentification), Linxens (smart cards), Fortinet (cyber products), and Econocom (cyber services)

The companies around the 50th position have digital trust sales in France amounting for €55 M approximately: Somfy, Securitas (Stanley Security), Serma Safety & security, Schneider, Honeywell, Palantir, Devoteam, SAP, Oracle, Bechtle, Inetum, Claranet, Computacenter, Scalian... Finally, although French players largely dominate the top 10 of the sector, there is a stronger presence of foreign companies established in France, US players in particular, among the top 10-50.

1.1 Cybersecurity and Digital Security: two complementary fields

Digital Trust is the guarantee of digital progress. Over the years, it has become a societal and industrial issue as important as the develoSMEsnt of digital technologies themselves, because it is a matter of how trustworthy these technologies, now at the heart of all our activities, are. For any individual or organisation, digital trust means the assurance that the digital systems that affect them are secure and that they will improve their physical, financial and image security, while at the same time protecting their private life and data (including personal data).

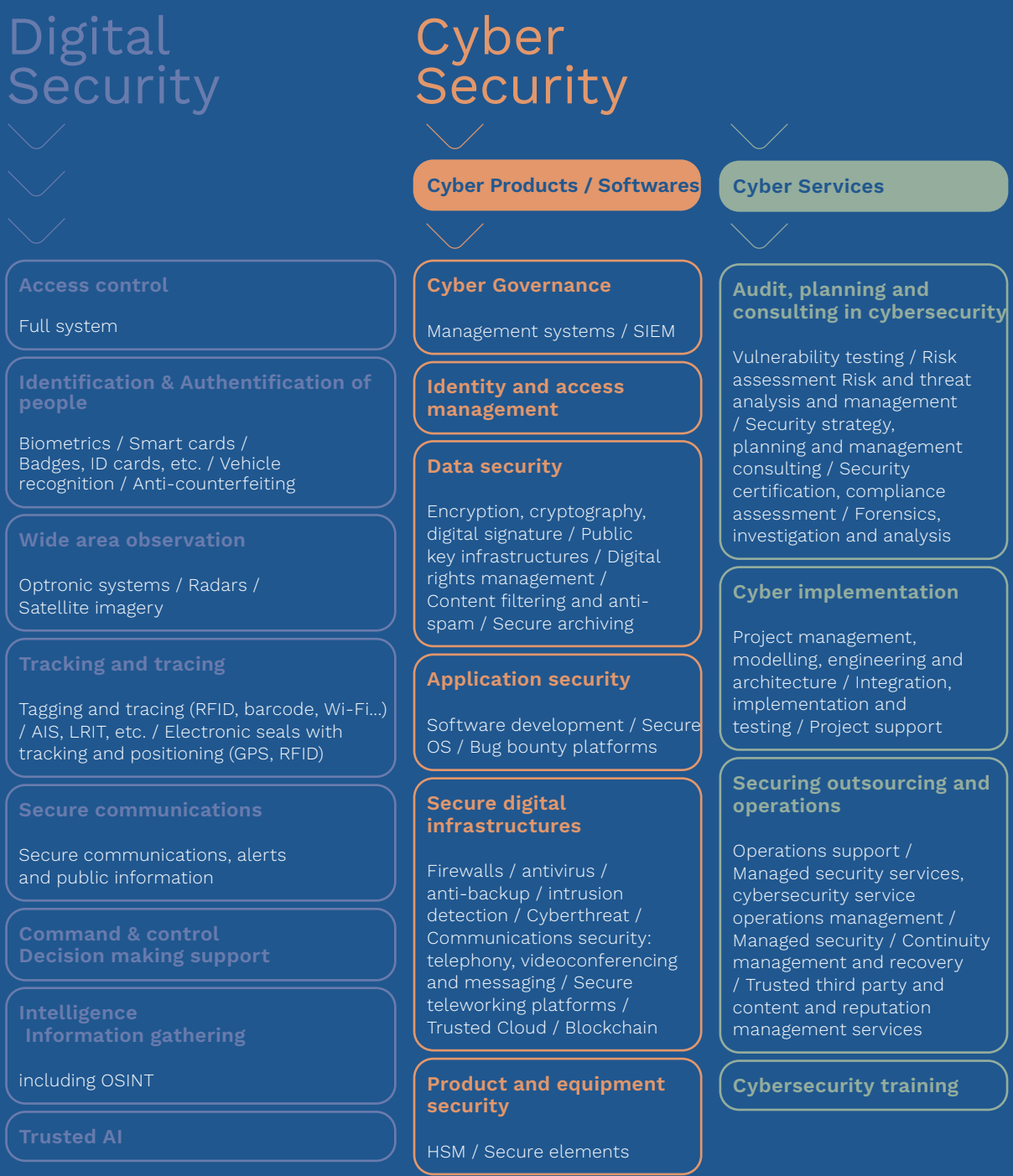
The **Observatory of Digital Trust** covers two industries:

1. **Cybersecurity**, which corresponds to the «internal» securing of digital systems. Cybersecurity brings together two types of activities that are often associated in practice: services (consulting, design, implementation, operation, training), and software & solutions, intended for the professional markets (State and public sector, critical installations, companies, SMEs) and the general public (computers, smartphones, homes, vehicles and connected objects, etc.)

2. **Digital Security**, i.e. electronic products and solutions for implementing digital systems to build trust in the outside world. These systems implement secure digital means to build trust in the citizen environment, in particular through identity management, access management, biometrics, transactions, connected objects and vehicles, industrial processes and logistics, transport, networks, smart cities, etc. Digital security products are hardware products (smart cards, documents, readers, etc.) or equiSMEsnt (access management, biometrics, detection, localisation, etc.).

1.2 The Scope of Digital Trust - Segmentation

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



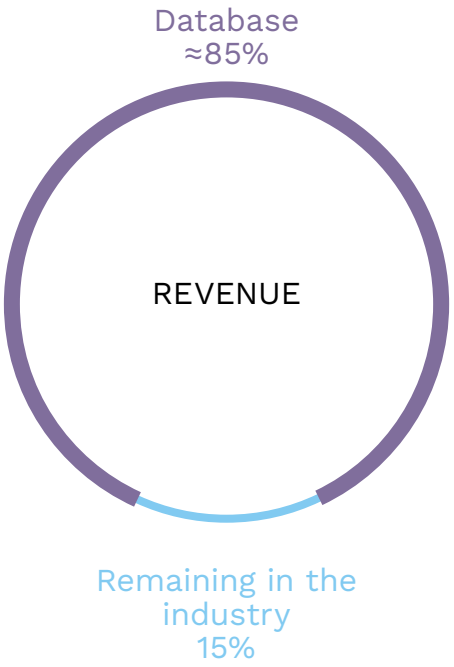
1.3 Methodology

This Observatory aims at both defining the perimeter of the industry and assessing its economic weight and characteristics.

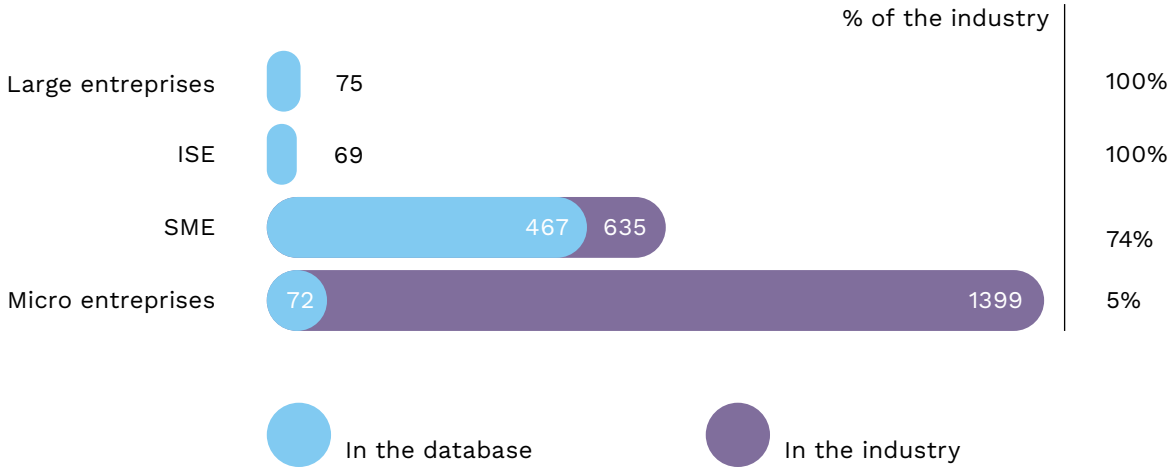
DECISION Etudes & Conseil has been conducting this Observatory since 2017. The data presented in this report are taken from a DECISION's database listing 683 companies out of the 2,178 that make up the Digital Trust sector. This database takes into account:

- All large entreprises in the sector (75/75);
- All the intermediate-sized entreprises (ISEs) in the sector (69/69);
- The majority of small and medium-sized enterprises (SMEs) in the sector (467/635);
- The most remarkable and innovative micro-enterprises and startups (72/1399).

Thus, although only 31% of the companies in the sector are included in the database, it is representative of 85% of the total revenue of the French Digital Trust industry.



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 2015-2023: 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 17 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 15 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 2024 edition, the members who answered the questionnaire represent 9% of the sector's revenue in France.

Finally, a specific analysis of the evolution of the global activity (global and security) of the main Digital Trust players is carried out each year to estimate the revenue achieved by the sector abroad and its evolution.

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.

As a result, the absolute figures of each edition of the observatory are not directly directly comparable. The figures of this Observatory are presented for the year 2023 and in accordance with the new segmentation of players. The updated 2022 figures are on page 13 of this report.

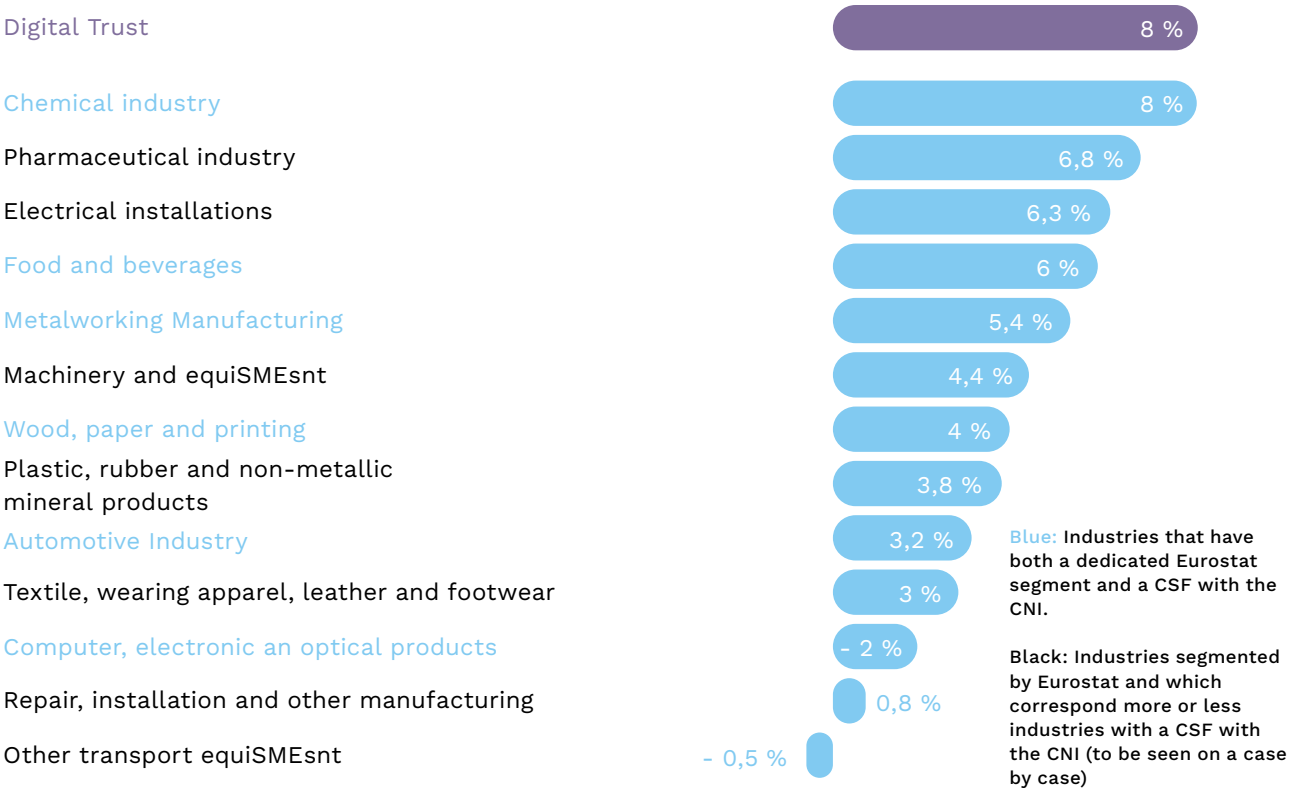
II) DIGITAL TRUST : AN IMPORTANT AND DYNAMIC INDUSTRY

2.1 Digital Trust is one of the fastest growing industries in France over the 2016-2020 period

Over the period 2016-2022, Digital Trust is one of France's fastest-growing industrial sectors, averaging 8%/year. Although measured using a method that is not directly comparable, the only other French industrial sectors enjoying similar growth are the chemical, pharmaceutical, electrical equiSMEsnt, food and beverage, and metal products industries. Other industries enjoy average annual growth of 0% to 5% over the same period, or even negative growth, as in the case of non-automotive transport equiSMEsnt.

Digital Trust is one of only four industries (out of a total of fifteen) not to have suffered a recession in 2020. With growth of 3.6% that year, it was the sector that best withstood the COVID crisis and its aftermath. This resilience reflects the long-term need for Digital Trust goods and services. As a result, by 2030, Digital Trust could become France's 11th out of 15 industrial sectors in terms of added value, overtaking both the electrical equiSMEsnt sector and the repair, installation and other manufactured goods sector.

Average annual growth of french industries over the 2016-2022 period

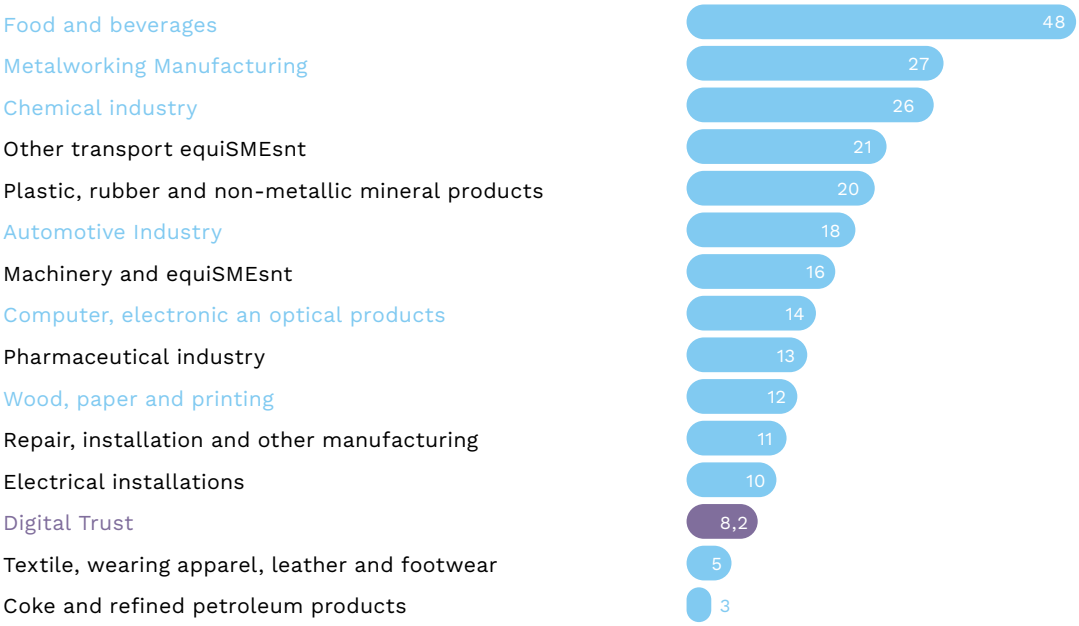


Source : DECISION, based on Eurostat data from 2016 to 2022

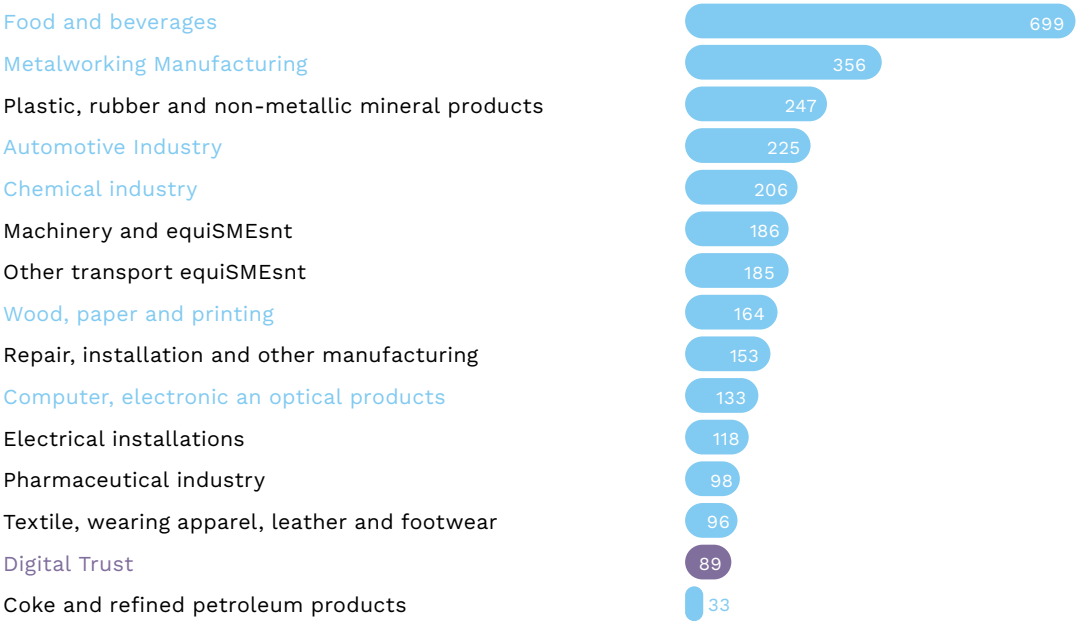
2.2 Digital Trust is a fully-fledged French industrial sector

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 to the electrical equiSMEsnt or wood, paper and printing sectors. In terms of employment, it is much larger than the coke and refined petroleum sector and is close to the textile and clothing sector.

Added values of the french industries in 2021 (€ Billion)



Workforce in french industries in 2021 (in thousands)



Blue: **Industries which have both a dedicated Eurostat segment and a CSF with the CNI.**
Black: Industries segmented by Eurostat and which correspond more or less to sectors with a CSF with the CNI (to be determined on a case-by-case basis)

Source : Decision, Eurostat, OCDE

2.3 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 47% (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.

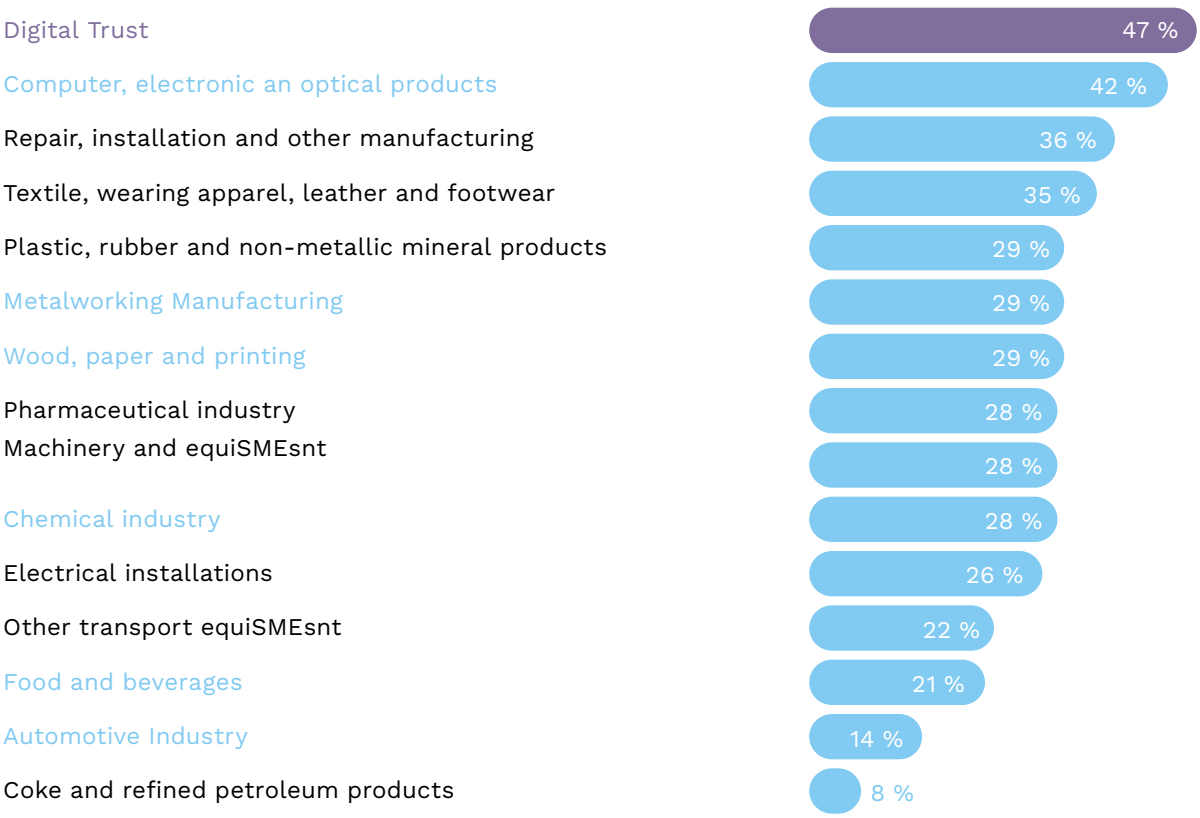
This phenomenon is mainly explained by three factors :

1. **The percentage of activity dedicated to services is relatively high in the French Digital Trust sector** (25% in 2023), 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. 2. Electronic products dedicated to Digital Trust (digital security) correspond to 45% 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, develoSMEsnt, 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. 3. Finally, cybersecurity products account for 30% of the total revenue of the security industry and involve **a very large proportion of highly qualified jobs** (software develoSMEsnt, etc.), associated with a very high rate of added value (at levels close to those of cybersecurity services).

Added value rate (added value/revenue) of french industry in 2021



Blue : Industries which have both a dedicated Eurostat segment and a CSF with the CNI.
Black: Industries segmented by Eurostat and which correspond more or less to sectors with a CSF with the CNI (to be determined on a case-by-case basis)

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 develoSMEsnt, **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 makes possible today**. France excels in particular in the following areas

Artificial Intelligence & Machine learning : France excels in deep learning. For several years now, the GAFAMs have set up research centres dedicated to this field and have been recruiting many French talents. France is also seeing the emergence of pioneering companies in generative AI, such as Mistral AI, which has become a French unicorn. On the public R&D side, INRIA has teams dedicated to defense and attack strategies using deep learning.

Cryptography : France has historically been one of the world leaders and is maintaining its position.

Post-quantum technologies (including cryptography) : France remains in the top three worldwide. In a few years, quantum computers should 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 the lack of staff dedicated to Big Data. France has nearly 1,000 full-time academic researchers working on cybersecurity issues, particularly on the Rennes, Paris-Saclay, 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 equiSMEsnt on a large scale and therefore contributes to a strong growth in volume of electronic security equiSMEsnt. In the short term, the growth of electronic components is cyclical and the 2020-2022 period was instead marked by a surge in semiconductor prices. Since the beginning of 2023, the decline in semiconductor prices has resumed its course.

2. **Digital transformation**. Accelerated by the COVID crisis in 2020, companies and administrations around the world are digitalizing their processes, deploying clouds and interconnecting data networks.

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

4. Finally, **numerous technological innovations** specific to the Digital Trust sector and in which France is often very well positioned both in terms of industrial players and scientific know-how: behavioural biometrics, innovations associated with secure elements, cryptographic develoSMEsnts, quantum computing, real-time analysis of wide-area observation data, blockchain, etc.

France has historically benefited from a powerful defence and security sector that exports strongly compared to the international average and has been able to take advantage of its excellence in research and develoSMEsnt to benefit from these four global trends and thus build a solid Digital Trust industry.
However, growth is even stronger in the US and especially Chinese digital trust industries.

2.6 Increasing compISEtion from foreign players

French players generate 74% of the Digital Trust revenue in France, i.e. €14.1 billion in 2023. In other words, foreign players in the sector generate 25% of the sector's revenue in France, i.e. approximately 5 billion euros in 2023. This figure corresponds solely to the revenue generated by the subsidiaries of foreign players in France and does not include exports by foreign players to France (which could not be measured in this observatory).

Although the share of wealth produced in France by French players is still fairly high, it has been falling steadily since 2013 and this trend is likely to continue. In particular, we have been witnessing for several years the develoSMEsnt of American players in France, notably through the installation of new 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... Chinese players are also developing, recently with high-level offers capable of compISEng on a technical level with French offers.

As for production in France, the weight of foreign players on the French market is significant: it is around 40%. In other words, the national market is still largely influenced by foreign and non-European solutions, whereas the French sector has offers in all segments and includes technological flagships and numerous players already capable of covering at least the entire national market.

Significant buyouts of French companies by foreign players took place in most of the Digital Trust segments over the 2013-2021 period. These include the takeover of Arismore by Accenture (USA), DenyAll by Rohde & Schwarz Cybersecurity (Germany), and Oberthur Technologies (bought by the US fund Advent in 2011) and then Safran Morpho (bought by Advent in 2018) then merged with Oberthur Technologies under the Idemia brand in 2018. Since 2021, however, the number and size of these buyouts has tended to decline, so that in 2022, the only takeover of a French company by a foreign company identified is that of Akka Technologies by the Swiss company Adecco.

Last but not least, many players in the Digital Trust sector suffers from a lack of a culture of purchasing French products, both from private companies and administrations. This lack of a culture of purchasing French products has naturally led French companies and administrations to turn to foreign offers. Indeed, in a general context of stagnating growth (1%/year growth in French GDP over the 2017-2022 period), and budgetary austerity on the side of public services, the first purchasing criterion often turns out to be the price. However, American and Chinese players are often more compISEtive than the French on the sole criterion of price (in particular because of greater economies of scale and greater subcontracting in countries with low wage costs). **In addition to penalising the French players in the sector, the purchase of foreign solutions that are not under control is likely to threaten France's sovereignty when the buyers are public bodies, OIVs (Operators of Vital Importance), and/or OSEs (Operators of Essential Services).** Despite the recent awareness of the issues of sovereignty and strategic autonomy, the lack of a culture of purchasing French products is particularly felt in the public sector and in large French companies.

The triptych of standardisation, certification and prescription, supported in particular by the ANSSI, makes it possible to guarantee the use of reliable and secure solutions while shifting the compISEtion from the field of price alone to that of technical excellence, thus naturally favouring the French players.

2.7 Conclusion - A sector with great potential if the right strategic choices are made

Digital Trust is a strategic industry because :

- The **growth** potential 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 **European 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.

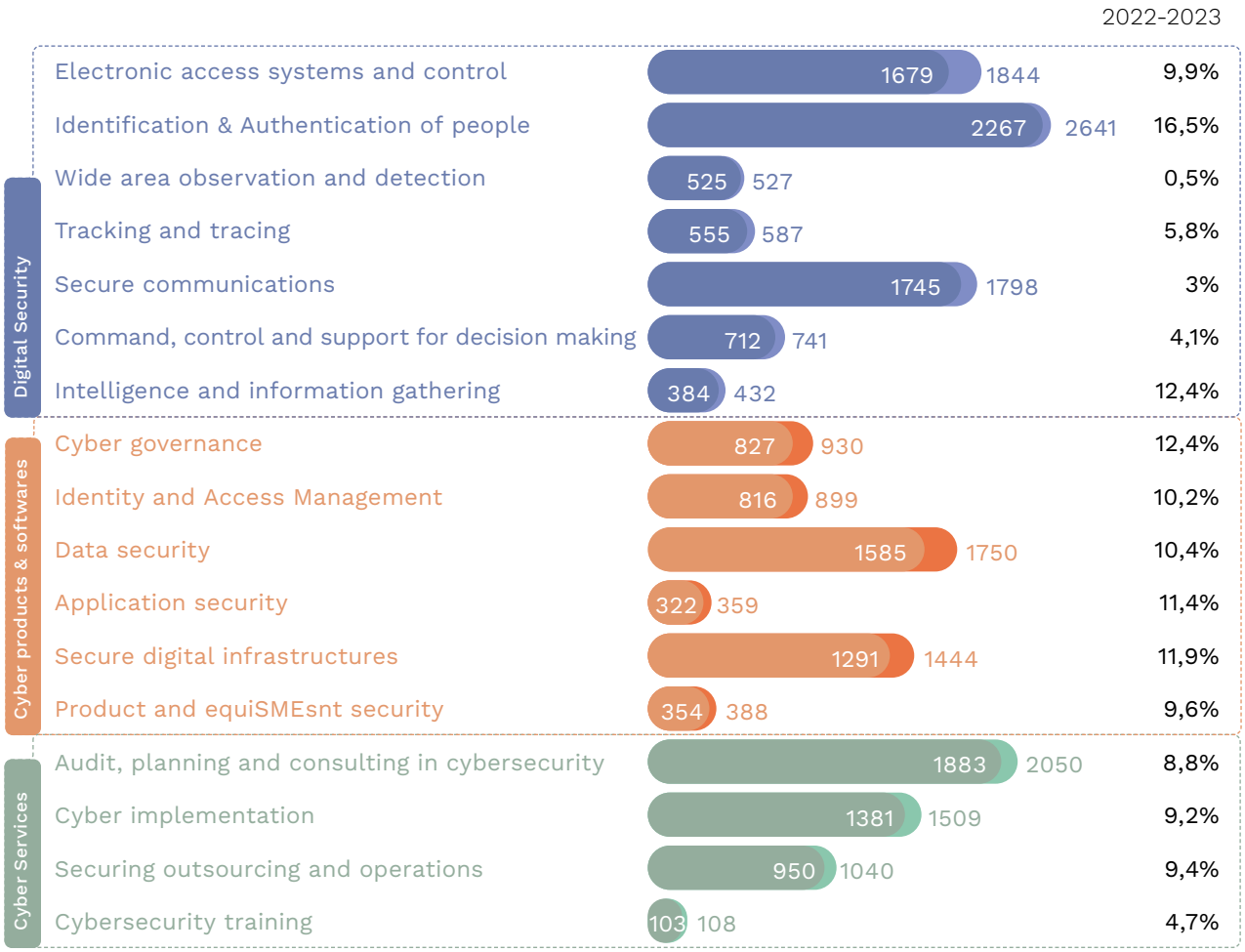
III

KEY FIGURES OF THE INDUSTRY

III. KEY FIGURES OF THE INDUSTRY

3.1 Size and growth

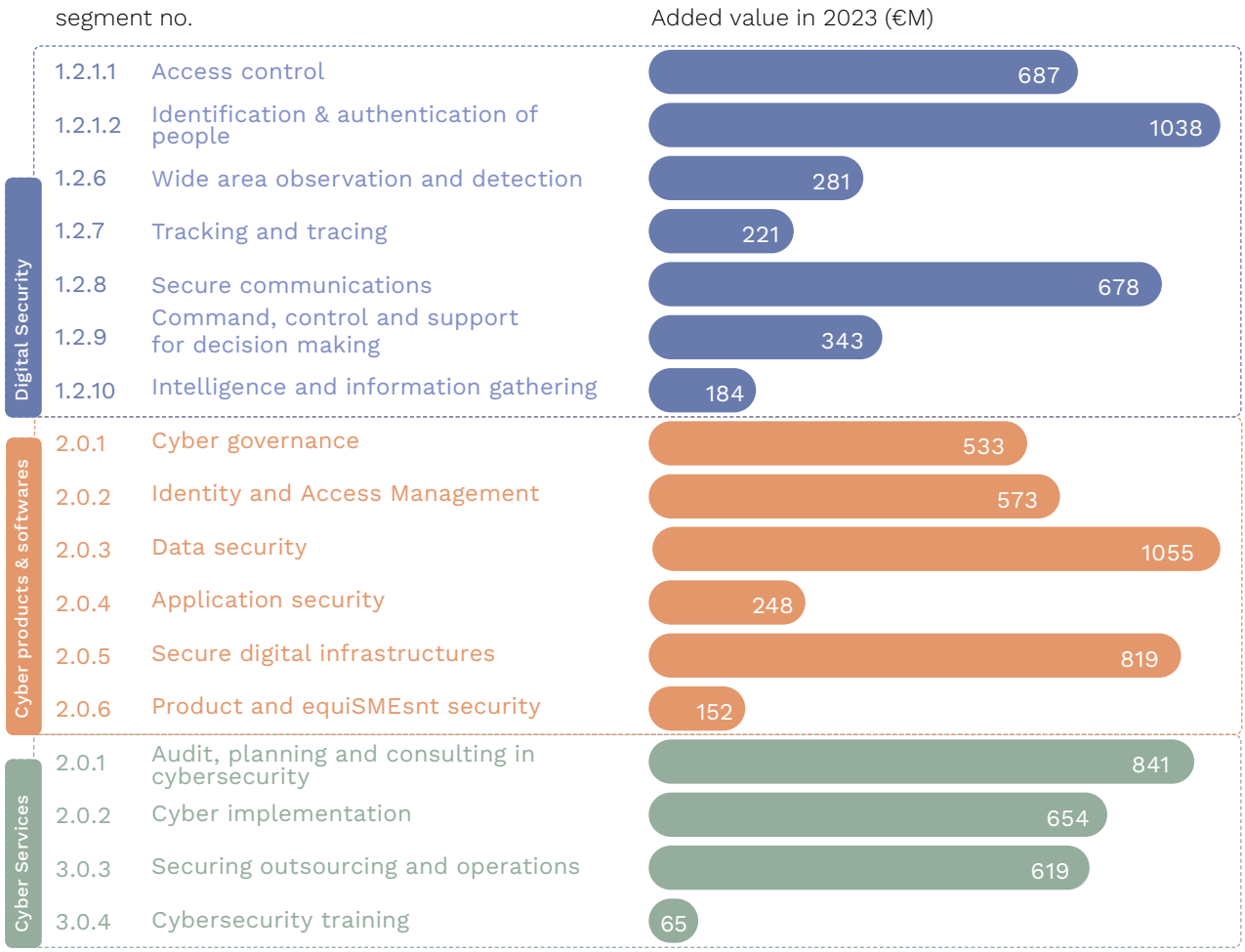
Revenue of Digital Trust in france € 19 B en 2023



Digital Security	Cyber products & softwares	Cyber Services	Total
+ 8,9%	+ 11,1%	+ 9%	+ 9,6%
€ 8 570 B	€ 5 570 B	€ 4 706 B	€ 19 045 B

3.2 Added value

Added value in France in 2023 per segment

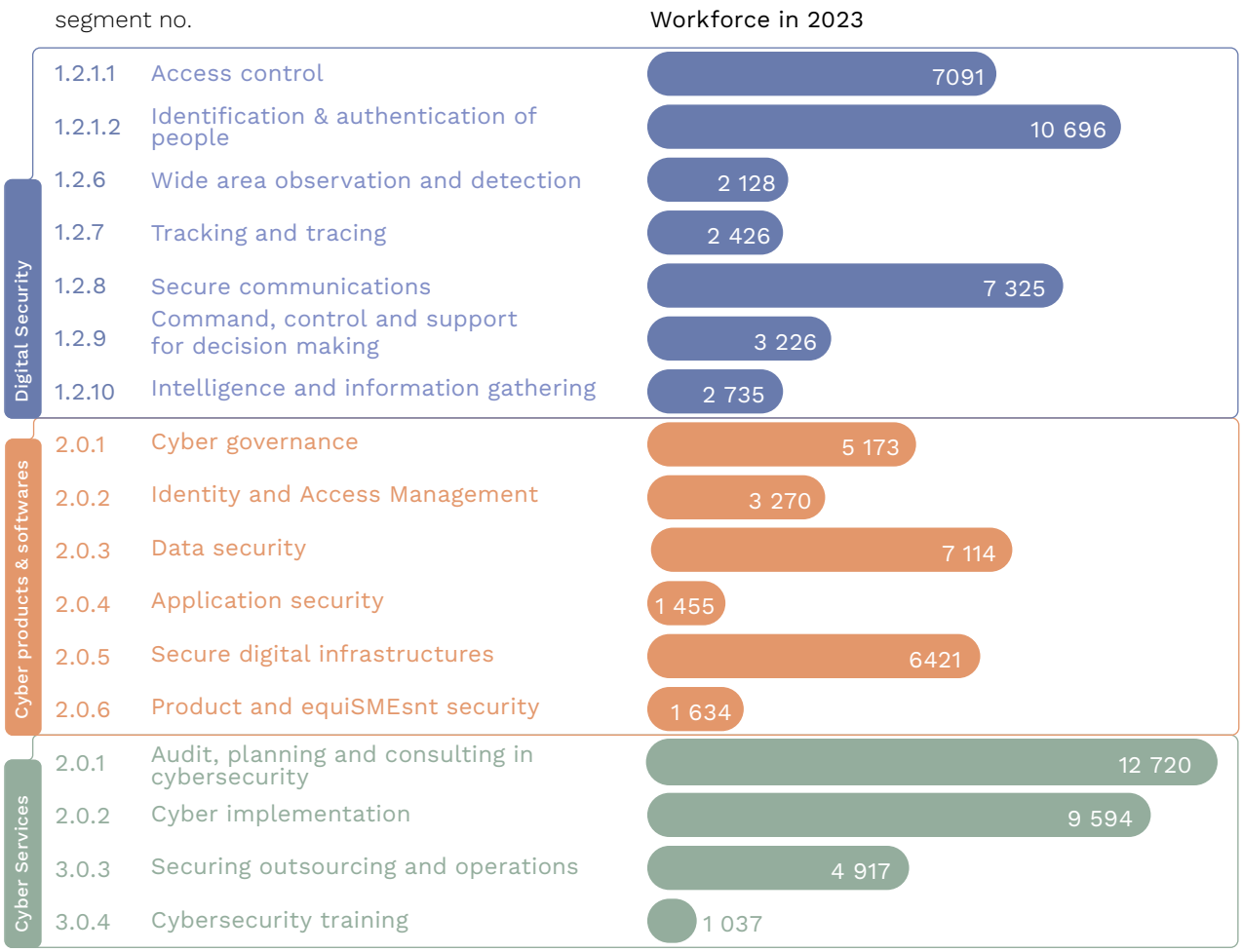


Digital Security	Cyber products & softwares	Cyber Services	Total
€3 432 M	+ €3 380 M	+ €2 178 M	= €8 990 M AV in digital trust in France

Source : Decision Etudes & conseils

3.3 Workforce

Workforcer in France in 2023 per segment

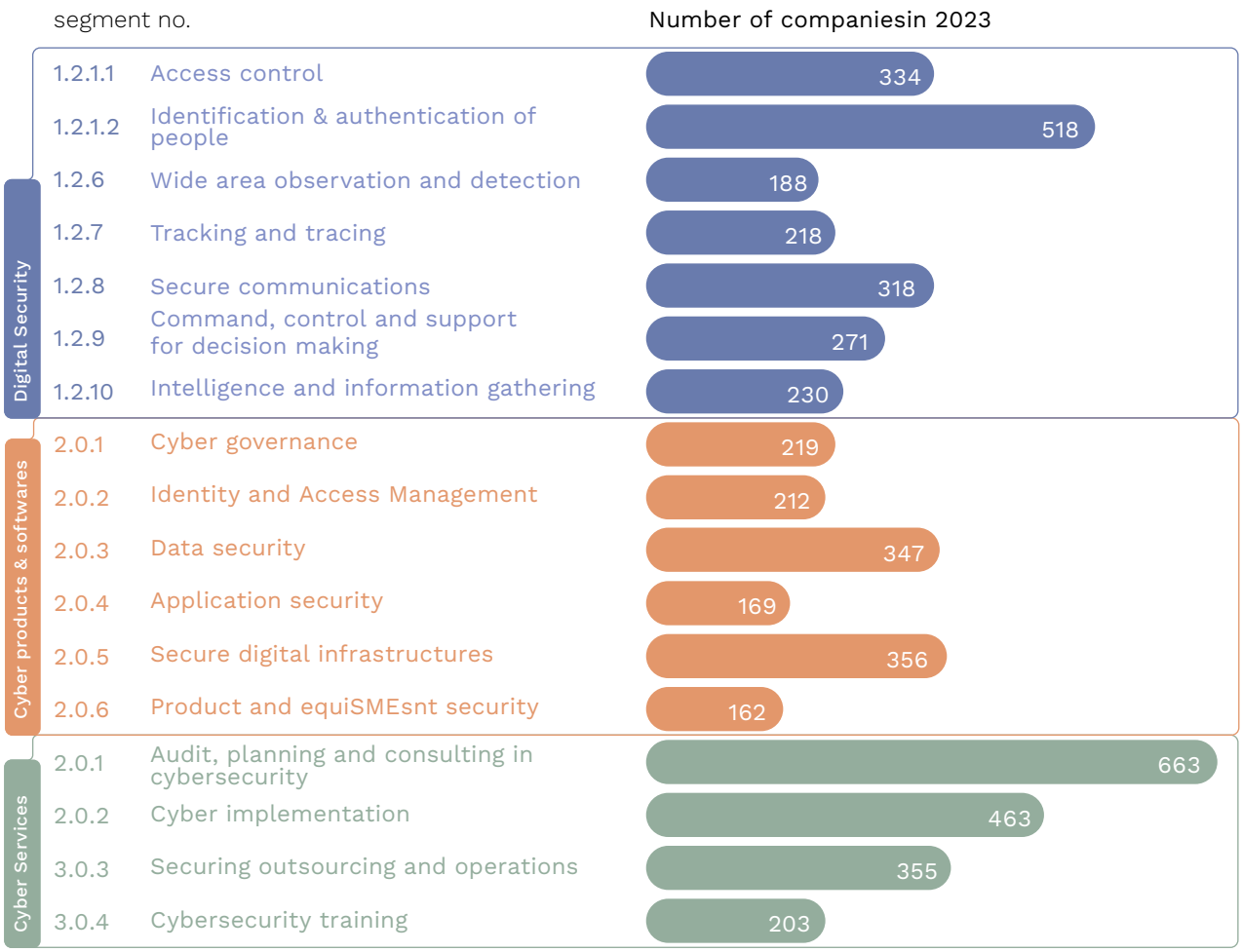


Digital Security	Cyber products & softwares	Cyber Services	Total
35 627 jobs	+ 25 069 jobs	+ 28 268 jobs	= 88 964 Jobs in Digital Trust in France

Source : Decision Etudes & conseils

3.4 Number of companies

Number of companies in france in 2023 per segment



Digital Security	Cyber products & softwares	Cyber Services	Total
1 775 companies	+ 726 companies	+ 704 companies	= 2 178 Companies in Digital Trust in France

Source : Decision Etudes & conseils

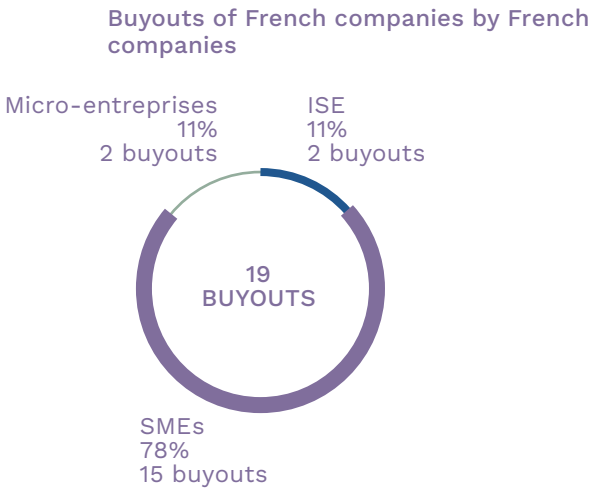
3.5 Mergers and Acquisitions

Company buyouts over the 2022-2024 period

Within the Digital Trust industry, 36 company buyouts concerning headquarters located in France have been identified from January 2022 to March 2024 (i.e. an average of 16 buyouts per year). These buyouts are both inter-company purchases and purchases of companies by financial funds and purchases between financial funds.

Among them:

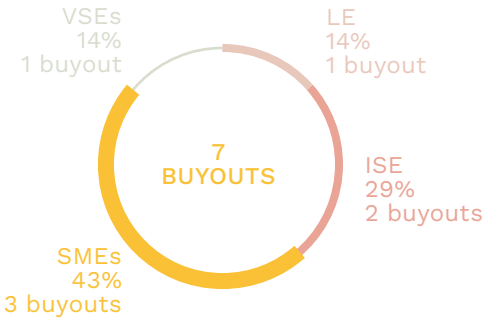
19 buyouts of French companies by other French companies (53%)



Source : Decision Etudes & conseils

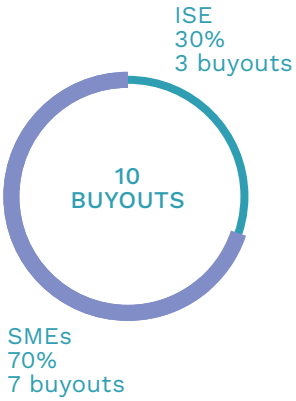
7 buyouts of French companies by foreign companies (19%)

Buyouts of French companies by foreign companies



10 buyouts of foreign companies by French companies (28%)

Buyouts of foreign companies by French companies



The vast majority of companies acquired are growing SMEs (69%).

Compared to the 2017-2020 period, the frequency of buyouts is similar, but the size of the companies bought out is on average relatively smaller, with a strong attraction for SMEs.

Moreover, over the 2017-2020 period, the number buyouts of French companies from foreign investments was significantly higher than the number of foreign buyouts from French companies, and for larger sizes of companies bought. This trend has faded and even reversed slightly since 2022, as shown by the buyout of Imperva and Tesserent by Thales in 2023.

In 2021, two-third of the buyouts of French companies by foreign companies were for the benefit of American investors, in line with the 2017-2020 period. These include Link by net, Openminded and AFD.TECH, all three of which were acquired by Accenture. Between 2023 and March 2024, the United States remained the main foreign acquirer of French companies, with 3 buyouts recorded: Brainwave GRC acquired by Radiant Logic, Proph3cy acquired by the Carlyle fund and finally Vade acquired by Hornetsecurity (a German company with American capital).

Finally, the major French groups have shown their interest in the European market since 2022 by buying up companies whose market is generally located in countries bordering France.

A. Main acquisitions since 2023 from the French Digital Trust leaders

Thales expands its worldwide activities through two strategic acquisitions

In 2023, Thales strengthened its position in the field of cybersecurity with several major purchases. Firstly, the company acquired Tesserent, an Australian company specializing in the protection against cyber attacks, for 111 million euros. Tesserent is renowned for its contracts with the public and defense sectors in Australia and New Zealand, and brought in around 110 million euros in revenues last year.

However Thales' biggest purchase was Imperva, a US company specializing in data and application security, for $3.6 billion. This acquisition is the fifth in just over a year for Thales and follows the purchases of S21sec, Excellium, and OneWelcome, signaling a major effort to become a global leader in cybersecurity. With the acquisition of Imperva, Thales hopes to add around 500 million euros to its cybersecurity sales, notably by expanding its activities in the US market, targeting a total of 2.4 billion euros per year.

Airbus strengthens its cybersecurity activities with the acquisition of Germany's Infodas

At the end of March 2024, Airbus acquired Infodas, a German company specializing in cybersecurity, marking a significant strengthening of its cyber portfolio. Based in Cologne, with 250 employees and annual sales of €50 million, Infodas stands out for its advanced security solutions for the public sector, defense and critical infrastructures. This acquisition, scheduled for completion by the end of 2024, underlines Airbus' commitment to positioning itself as a leader in critical systems protection, especially in the context of the development of the Future Combat Air System (FCAS).

Chapsvision continues its aggressive external growth strategy

ChapsVision is actively pursuing its external growth strategy to become an European leader in the sovereign processing of massive, heterogeneous data. Through key acquisitions, ChapsVision is strengthening its expertise and expanding its portfolio of solutions. Following several acquisitions aimed at expanding its cyber portfolio by 2022, the group has been developing its cyber intelligence skills since 2023.

These acquisitions include Geotrend, a specialist in economic and strategic intelligence; ACIC, a Belgian expert in video processing using artificial intelligence, strengthening ChapsVision's capabilities in intelligent video surveillance, meeting the security needs of businesses and public administrations; and Owlint, a start-up specializing in open source intelligence (OSINT). These acquisitions complete ChapsVision's offering by integrating advanced technologies for web data analysis, strengthening cybersecurity and business intelligence. These acquisitions reflect ChapsVision's ambition to create a European leader in cyber intelligence and cybersecurity, confirming its commitment to the EU data sovereignty.

Docaposte consolidates its leading position in the healthcare market

Docaposte strengthens its position in the healthcare sector through strategic acquisitions designed to complement its offering of digital trust solutions and services. In particular, Docaposte has acquired Thiqa, a specialist in digital trust and security services, which strengthens Docaposte's offering in consulting, integration and operations. The addition of Weliom, a consulting firm with expertise in healthcare, broadens Docaposte's skills in digital strategy, information systems security and compliance. Finally, Docaposte completes its security-related acquisitions with Maincare and Axonal-Biostatem, a healthcare software publisher and a leader in clinical research and development. Combining these expertises with Docaposte's digital trust capabilities will make Docaposte a sovereign technology leader for the digital transformation of the healthcare sector.

B. The main acquisition of French companies by foreign investors

The United States remains the main buyer of French companies between 2023 and today

Three acquisitions by American capital were recorded during this period. Firstly, Radiant Logic acquires Brainwave GRC, a French specialist in identity data. This acquisition enables them to strengthen their mutual capabilities by offering an integrated platform for identity data governance and near-real-time behavioral analysis, contributing to better detection of cyber-attacks and fraudulent activities.

Next, US investment fund Carlyle acquires Pr0ph3cy, a French cybersecurity start-up. Carlyle's investment of almost 100 million euros is intended to support Proph3cy in its expansion through acquisitions. Proph3cy was renamed Neverhack after this acquisition.

Finally, Hornetsecurity, a German company with a majority of American capital, acquired Vade, a French specialist in e-mail security, impacting French sovereignty. This acquisition enables Hornetsecurity to strengthen its e-mail protection offering and extend its presence on the French market.

Sale of Thales IoT business to newly formed Telit Cinterion

In the third quarter of 2022, Thales has reached an agreement to sell its cellular IoT products business, initially acquired when Gemalto was acquired in 2019, to Telit, which will thus create Telit Cinterion. This new entity aims to become a Western leader in IoT solutions. In this transaction, Thales receives a 25% stake in Telit Cinterion, now controlled by UK-based DBAY Advisors. This sale enables Thales to focus more on industrial IoT, while retaining a strategic interest in Telit Cinterion.

Bechtle acquires Apixit and enters the French cybersecurity market

Formerly close to the top 50 companies in the French digital trust sector, Apixit, a French cybersecurity services company, has been acquired by Bechtle, a leading German IT services company. The acquisition marks Bechtle's entry into the French cybersecurity market, and strengthens its position as one of France's leading IT players.

3.6 A dynamic year for fundraising

As a sign of the attractiveness of the sector, the number and amount of funds raised by Digital Trust startups has continued to grow exponentially over the past six years.

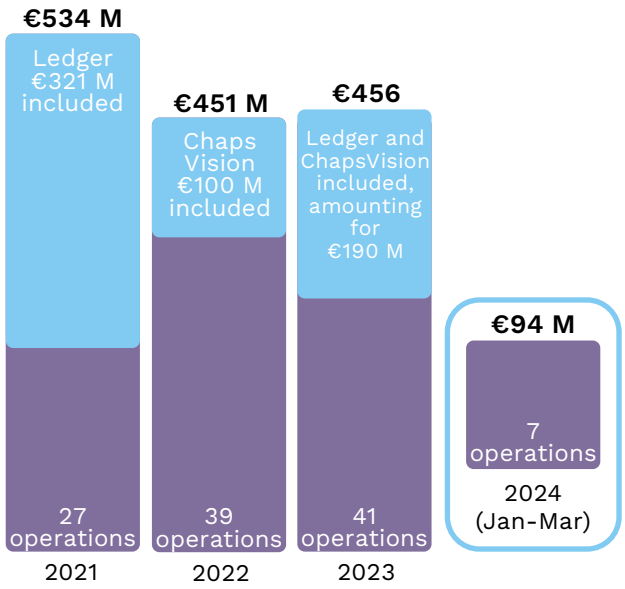
As shown in the infographic below, 41 fundraisings were carried out within the industry in 2023, representing a total amount of 456 million euros. The period from January to March 2024 shows a positive momentum in fundraising, with already more than €94 million raised through 7 transactions, Zama standing out with a €73 million round.

For the third year in a row, the industry benefited from exceptional fund-raisings in 2023: €100 million for Ledger and €90 million for ChapsVision, two companies that had already received major investments in previous years.
Out of a total of 456 million euros, ACN members accounted for 36% of investments, or 166 million euros in 2023. In the first quarter of 2024, out of a total of 94 million euros invested, ACN accounted for 84% of investments, thanks to operations led by Zama and Anozr Way.

In 2023, the vast majority of companies were backed by French investors, including major players such as Tikehau Ace Capital, Qualium Investissement, InfraVia Capital, Banque des Territoires, Crédit Mutuel, 115K, etc.

Despite a difficult economic climate in 2023, less favorable to investment, France has maintained its previous momentum, with the number of deals still higher than in previous years, and the total amount surpassing that of 2022. France retains its place on the European continent podium for fundraising in the Digital Confidence sector, ranking second in terms of number of deals and amounts raised, and third in terms of average amount raised. This position is all the more significant for the industry and for France, which is demonstrating remarkable resilience. According to the 2024 European cybersecurity investment barometer by Tikehau Ace Capital, amounts raised in Europe, across all sectors, have fallen due to a less favorable economic and financial context. Although the number of funds raised increased, the total amount raised by the European cybersecurity sector fell by 42% in 2023. This downward trend, to which France is an exception, can also be observed in the USA and Israel.

Amount of funds raised by French Digital Trust startups



List of fundraising activities of French Digital Trust startups

In 2022

	Company	Organization	Year	Amount (M€)
1	ChapsVision	ACN	2022	100
2	Mailinblack		2022	50
3	Tehtris	ACN	2022	44
4	Zama	ACN	2022	43
5	Vade		2022	28
6	Gatewatcher		2022	25
7	Trustpair		2022	20
8	Crowdsec	ACN	2022	14
9	DFNS		2022	12,3
10	Citalid	ACN	2022	12
11	Hackuity		2022	12
12	Stoïk	ACN	2022	11
13	Secure-IC		2022	10
14	Yogosha	ACN	2022	10
15	Bodyguard		2022	9
16	Dattak		2022	7
17	Cosmian		2022	4,2
18	Bfore.ai		2022	4
19	Stoïk	ACN	2022	3,8
20	Ocode		2022	3
21	Meelo		2022	3
22	Augmented Ciso		2022	2,5
23	ncScale		2022	2,5
24	C-risk		2022	2,5
25	Arsen		2022	2,5
26	Buster.ai		2022	2
27	Patrowl		2022	2
28	Snowpack		2022	2
29	Tenacy		2022	1,6
30	Equisign		2022	1,6
31	RFence		2022	1,3
32	Cryptr		2022	1,2
33	Kubo Labs		2022	1
34	Dastra		2022	1
35	Legapass		2022	1
36	Cyberjobs		2022	0,9
37	dappy		2022	0,5
38	Ravel		2022	
39	Eyst		2022	
	Total ACN			238

In 2023

	Company	Organization	Year	Amount (M€)
1	Ledger		2023	100
2	ChapsVision	ACN	2023	90
3	DataDome		2023	38,6
4	sekoia.io	ACN	2023	35
5	Egerie		2023	30
6	HarfangLab		2023	25
7	Provenrun		2023	15
8	Dattak		2023	11
9	CryptoNext		2023	11
10	Sesame IT	ACN	2023	10
11	Stoïk	ACN	2023	10
12	Cybervadis		2023	7
13	Ecole 2600	ACN	2023	6
14	Filigran		2023	5
15	MiTrust		2023	5
16	Astran	ACN	2023	4,7
17	Qevlar AI		2023	4,5
18	NANOCORP	ACN	2023	4,2
19	CSB school		2023	4
20	VSORA		2023	4
21	OverSOC		2023	3,8
22	Escape		2023	3,6
23	Narval		2023	3,6
24	Zygon		2023	2,8
25	Dotfile		2023	2,5
26	Bastion Technologies	ACN	2023	2,5
27	elba		2023	2,5
28	ShareID	ACN	2023	2
29	Defants		2023	2
30	Alcyconie		2023	2
31	VeriCloud		2023	1,9
32	Qontrol	ACN	2023	1,5
33	Naaia		2023	1,3
34	Mithril Security		2023	1,2
35	BonjourCyber	ACN	2023	1
36	Legapass		2023	0,6
	Inspeere		2023	0,6
37	Escape		2023	0,5
38	OneWave		2023	0,4
39	Bastion Technologies	ACN	2023	
40	Kubo Labs		2023	
	Total ACN			167

3.7 The emergence of a strong ecosystem of Digital Trust Micro-entreprises

As shown in the infographic below, the French Digital Trust ecosystem is built around **large historical players**, often from the digital security and/or digital services sectors, and often linked to the sovereign and defence ecosystems. These major historical players, who are strong exporters, have offers geared towards governments, Operators of Vital Importance (OIVs), and large international companies. They represent €15.7 billion in revenue in 2022.

However, **an ecosystem of Micro-entreprises specialized in Digital Trust** started to emerge in the 1990s. During the decade of the 2010s, this ecosystem gradually grew in importance and now includes many large SMEs, some of which have already exceeded the €50M revenue mark and have become Intermediate Size Entreprises (ISEs) with an international focus. This ecosystem is composed mainly of cybersecurity startups, many of which have offers aimed at addressing new markets such as Micro-entreprise/SMEs and small local authorities. The strong growth of this ecosystem is driven by fund-raising for increasingly large amounts year after year. This ecosystem represents an estimated revenue of between €2.5 and €3 billion in 2022 (adding together Micro-entreprises with a revenue of more than €5 million, companies that have raised funds of €5 million or more, and Micro-entreprises that have become ISEs since 2000).

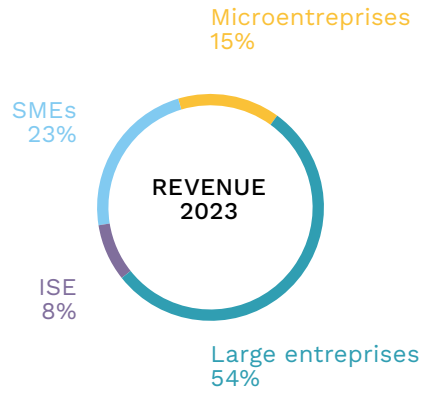
Emergence of a strong ecosystem of SMEs

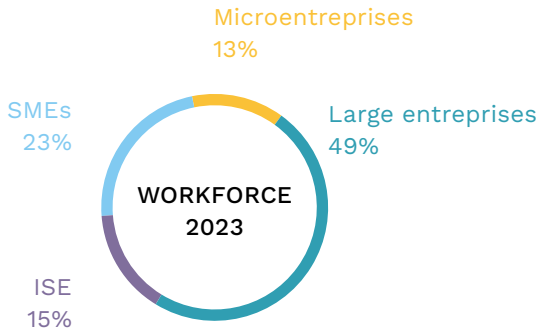
€2,5 to €3 B in 2023

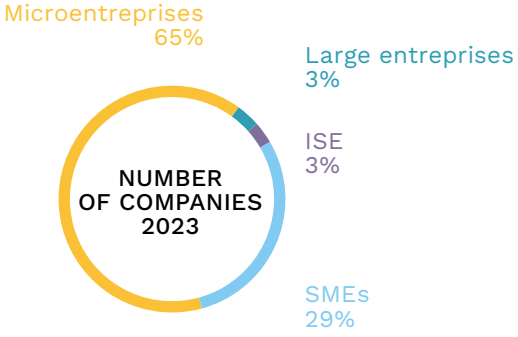
Major historical players

€15,7 B in 2023

Analysis by company size







IV. CURRENT STATUS OF ONLINE THREATS

4.1 The threat as seen by ANSSI

In its Panorama 2023, the ANSSI (Agence Nationale de la Sécurité des Systèmes d'Information) looks back at the major trends observed in 2022-2023 and proposes a short-term outlook.

The ANSSI has once again noted an increase in computer threats, higher than in 2022, particularly computer espionage and ransomware attacks. One of the reasons for this development is the geopolitical context marked by high tensions and the holding of events on French soil, such as the 2024 Olympic and Paralympic Games.

Trend :
30% ransomware attacks in 2023

2022 :
832 proven incidents

2023 :
1112 confirmed incidents

Reference Document :
Cyber Threat Panorama 2023
ANSSI - 27 February 2024

Document available below:
https://www.cert.ssi.gouv.fr/uploads/CERTFR-2024-CTI-001.pdf

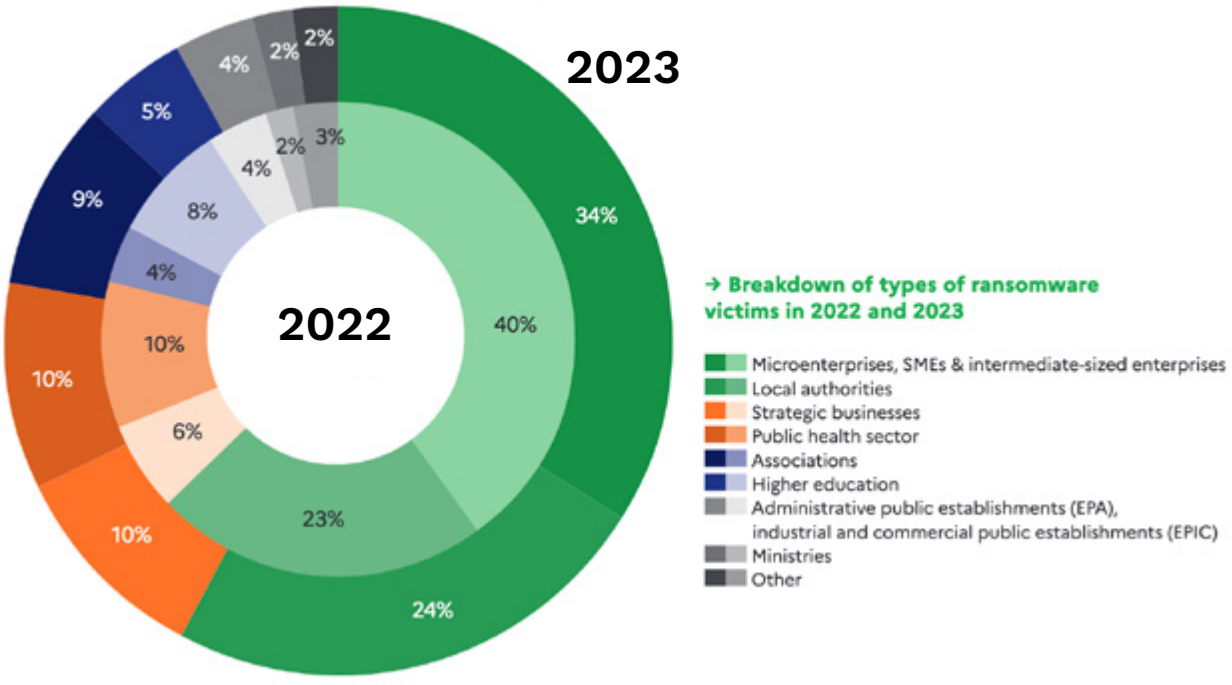
1. A significant increase in the cyber threat

There has been a sharp increase in the cyber threat in France compared with 2022. Computer espionage remained at a high level in 2023, with attacks mainly affecting individuals and non-governmental organisations that may create or host sensitive data.

ANSSI noted that espionage via professional and personal mobile phones, aiming targeted individuals, had increased. The same observation applies to attacks designed to promote a political discourse, hinder access to online content or damage an organisation's image.

Ransomware attacks on French organisations accounted for 30% of computer attacks in 2023. In the health and energy sectors, whose entities are particularly sensitive to service interruptions, cybercrime still represents a major threat. The ANSSI supported an international operation to dismantle the infrastructure of the QaKBot cybercrime network.

The graph below shows the evolution of targeting by ransomware through incidents handled by the ANSSI in 2022 and 2023. The ANSSI has noted an increase in attacks affecting the associative sector and local and regional authorities:



Source : ANSSI, 27 February 27, 2024, «Cyber Threat Panorama 2023»

2. The constantly evolving offensive capabilities of malicious actors

Malicious actors are constantly improving their offensive techniques. Their main objective is to reduce the risk of being detected via more discreet and complex anonymisation networks. The tools used to carry out an attack are becoming ever more performant.

At the same time, the ANSSI observed that certain routers used by private individuals, small and medium-sized enterprises (SMEs) or local authorities, are compromised and then integrated into anonymisation networks. These routers are then used as active relays for espionage campaigns and, more broadly, cybercrime.

In addition, peripheral equipment (routers, email gateways, firewalls, etc.) are still a vulnerability for IT systems in 2023. The ANSSI has noted that living-off-the-land techniques (exploitation of applications and functionalities already present on the compromised network) have been particularly used by cybercriminals, making it more difficult to distinguish between the activities of the attacker and those of the victim. The ANSSI points out that these techniques have been used by Russian and Chinese attackers on infrastructures in the United States and Ukraine.

In addition, the private surveillance market has seen a real boom, with some companies supplying malicious code to public bodies, businesses, or private individuals with the intention of causing harm. To combat the proliferation and misuse of commercial spyware, France supported the Joint Declaration adopted at the 2nd Summit for Democracy. Moreover, at the Paris Peace Forum in November 2023, both United Kingdom and France held consultations to combat the development of commercial spyware.

3. Better selected attack opportunities

Malicious actors are now using more specific weaknesses to compromise the IT systems they target. The flaws can be both technical and human: exposure of unsecured equipment on the Internet, poor administration or management practices, vulnerabilities in systems, lack of hardening, etc. These flaws provide attackers with loopholes through which they can penetrate, as victims have difficulty controlling their information systems.

The ANSSI dealt with numerous security incidents involving the exploitation of vulnerabilities during 2023, with the use of several 0-day or day-one vulnerabilities by cybercriminal groups. Messaging services were particularly targeted during that year: they enable attackers to access confidential company data or to break into their targets' workstations.

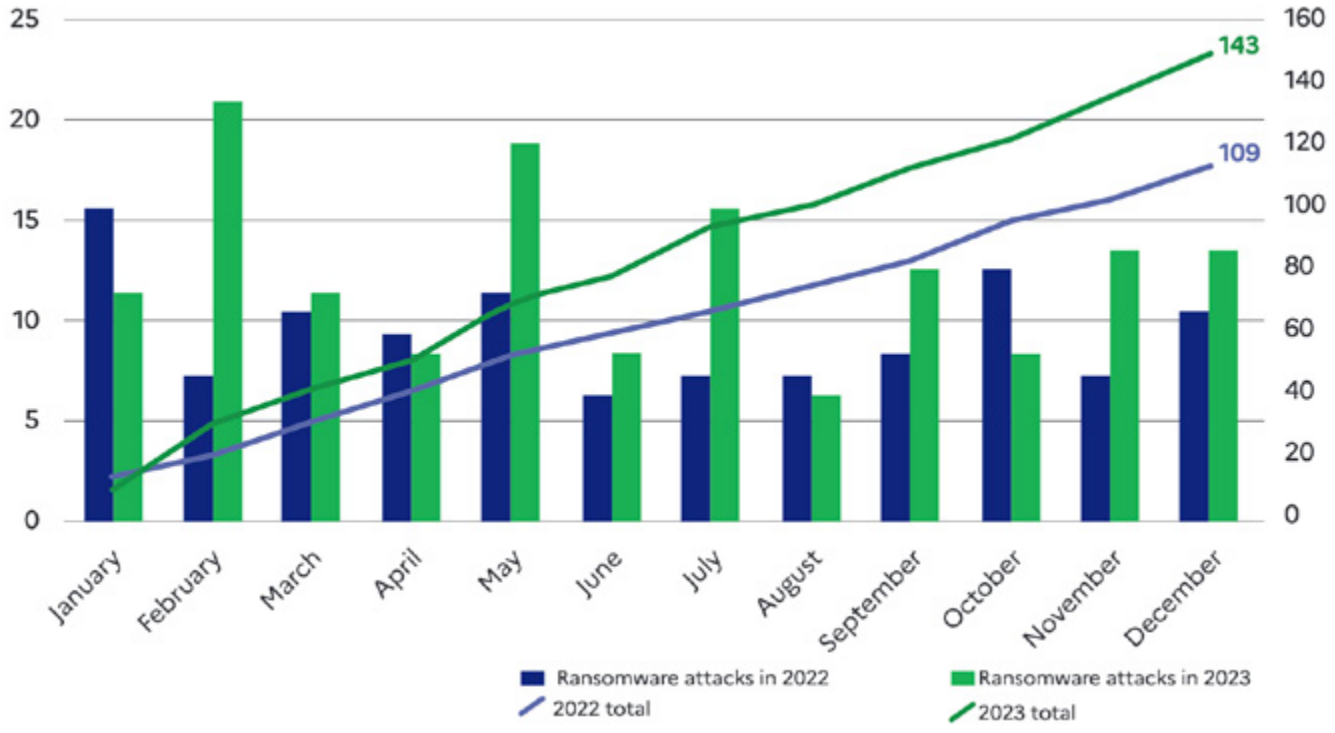
The opportunity for attackers to act is also found in the organisation of major events. A multitude of players are involved in organising these events, leading to varying levels of security. Exploiting the media coverage of the event, the organisers or the participants can represent ideal targets. Indeed, the Rugby World Cup organised in France in 2023 enabled the country to anticipate potential attacks in the run-up to the 2024 Olympic and Paralympic Games.

However, an espionage operation or distributed denial of service (DDoS) attacks could target the 2024 Olympic and Paralympic Games. To avoid it, the ANSSI will be heavily mobilised in the cybersecurity of this event. An IT security detection, alert and processing system will be set up in cooperation with the various government departments involved.

The international climate is still very tense, providing an opportunity for malicious actors to penetrate and maintain critical networks such as energy, transport, and logistics. Ukrainian entities remain one of the main targets, but pre-positioning activities have been detected in Europe, North America, and Asia.

Finally, over the course of this year, developments in the structure and methods of attackers show that the threat of large-scale attacks cannot be ruled out. For this reason, regular monitoring of CERT-FR publications on threats and vulnerabilities, together with the entry into force of the NIS 2 Directive, will enable us to progressively strengthen and guarantee a good level of cybersecurity.

Title of graph: Comparison of ransomware attack reports in 2022 and 2023:



Source: ANSSI, 27 February 2024, 'Panorama de la cybermenace 2023'.

4.2 Perspectives from industry experts

Back-up is dead, long live cyber resilience!

Yosra Jarraya
General Manager and co-founder

« Ransomware, a scourge that cripples' businesses, now strikes every two hours. The question is no longer «if» an attack will occur, but «when»! In the face of this threat, Survival Kits are becoming essential to guarantee organisational resilience. These kits complement the traditional business continuity plan (detection, containment, analysis, eradication, and restoration of back-ups), which takes between 22 and 90 days to complete. During this period of crisis, businesses cannot afford to simply 'wait it out'. The carefully selected data and services in these kits, which are continuously available, represent the last line of defence against the destructive financial impact and loss of customer confidence.»

Contextualising the threat to anticipate and quantify cyber risk

Alexandre Dieulangard
General Manager and co-founder

« 2024 will be the scene of a combination of geopolitical events and cyberthreats. Hacktivists exploit international tensions, as in Ukraine and in the Middle East, to carry out unsophisticated but high-profile actions. Despite the success of international blocking operations, cybercrime remains the main threat for public and private players. Discreet state actions remain a reality as shown by the recent reports on Sandworm, APT29 and Volt Typhoon. The Olympic Games will be a catalyst for attackers with a variety of motivations. In this context, the use of a Cyber Risk Quantification (CRQ) tool, supplied with reliable strategic intelligence, is essential if we are to face up to the cyber risk with trust and serenity.»

Ransomware becomes more professional

Erwan Keraudy
CEO and Co-founder

« Ransom demands are up by 40%, mainly due to the development of RaaS. In 2023, thanks to its ability to detect external threats, CybelAngel identified 62 active ransomware groups involved in more than 5,000 known attacks and 132 countries. Ransomware incidents are under-reported as more and more companies choose to pay the ransom and assume the associated risks rather than tackle the underlying problem. Yet identifying vulnerabilities early on can significantly reduce the threat. Ransomware-as-a-Service (RaaS) is growing in popularity, with more and more data, cloud services and databases being exposed. There is every reason to believe that this trend will continue to grow.»

Protecting everyone, a fundamental challenge

Gwenaëlle Martinet
Director of Cyber Offerings

« The largest organisations are now fully aware of the cyber risks and are deploying resources to protect themselves. Smaller organisations, whether in the private or public sector, face several difficulties: lack of human and financial resources, technical complexity that is difficult to grasp, and an abundance of solutions. Yet 20% of organisations have already fallen victim to cyberattacks. The challenge is therefore to democratise access to cybersecurity. Docaposte, France's leading provider of digital trust services, supports small and medium-sized organisations by integrating all the cybersecurity products they need to prepare, protect, and respond into a single contract. In this way, Docaposte enables everyone to deal with the threat simply and effectively. »

Increasing threats to mobile phones

Romain Waller
General Manager

« We are facing an increase in incidents of compromised mobile phones. New techniques are targeting mobile phones with increasing precision, for the purposes of espionage, cybercrime, or destabilisation. Mobile phones contain internal information and give access to a microphone close to the user, but they are also a possible vector of attack against an organisation's information system, as mentioned in the ANSSI's 2023 Panorama of the Cyberthreat. Following the Pegasus episode, traces of surveillance software were recently discovered in the mobile phones of members of the European Parliament. Faced with these challenges, it is imperative to put in place effective protection and detection measures to enhance security. »

Cloud, towards pragmatic and secure sovereignty!

Fanch Francis
CEO

« In 2023, the EU's digital autonomy is threatened by the dominance of the cloud giants, with AWS, Azure and GCP controlling more than 70% of the market. This foreign dominance exposes European businesses to risks linked to compliance and security, hampering data sovereignty. NANO Corp. is responding to this challenge by offering a control system that can be deployed on all clouds, including US hyperscale's, aligned with EU security certifications, to guarantee integrity and operational autonomy within the cloud. As the EU aims to increase its adoption of the cloud by 2030, our mission becomes crucial: to enable a secure transition to the cloud, thereby strengthening Europe's strategic position in the global digital arena. »

Growing adoption of strong authentication

Bruno Bernard
CEO

« Given the proliferation and sophistication of cyberthreats, the security of digital data is crucial. According to cybermalveillance.gouv.fr data for 2023, phishing remains the main threat to all users. To counter these attacks, double authentication by SMS is no longer sufficient. For optimum security, we recommend using strong authentication methods such as FIDO devices. This standard has been adopted by Microsoft, Google, Apple and more than 250 other service providers, including identity federations such as Evidian, Ilex, Systancia, Octka, Ping Identity, etc. .»

The rise of digital identity: a step forward for citizens, but also a breeding ground for fraud

Frédéric Cercle
General Manager

« The development of digital identity simplifies online interactions for EU citizens, yet also introduces a host of new risks and challenges. Electronic identification means (eID) creation relies on official identity documentation. Remote identity proofing for eID creation must, therefore, possess the capability to defeat deepfake and video injection attacks. With the current surge in AI-based technologies, fraudsters gain access to sophisticated tools for crafting deepfakes and synthetic identities. Combatting attempted biometric fraud emerges as a major concern to uphold the credibility of the digital identity market, pending enhancements announced in the eIDAS 2 regulation... »

Is Compliance the Key to Reducing Cybersecurity Risks?

Roland Atoui
CEO

« In 2023, a study by Cybersecurity Ventures revealed that 1 cyber-attack occurred every 39 seconds, totalling more than 2K cases per day. By 2022, Statista reckons 12 million IoT attacks, with the manufacturing and financial sectors taking the hardest hit. Europe has also suffered, with 4K+ incidents. As part of this global and European effort, standards, and regulations such as ETSI EN 303 645, CEN-CENELEC and CRA are working to ensure the necessary state-of-the-art security harmonisation. In the meantime, security relies on the personal initiatives of manufacturers and buyers of IoT products. It is with this in mind that CyberPass has been designed, to support these initiatives and simplify compliance. Faced with these challenges, what are you doing to secure our digital future? »

The cybernetic threat

Audrey Amedro
CEO

« In 2024, the cybernetic threat is becoming increasingly insidious and silent. These attacks, often undetectable until it's too late, exploit security loopholes to embed themselves deep within the network infrastructure. Faced with this type of cyberthreat, the adoption of a network detection system (NDR) becomes essential. Sesame*it's JIZÔ NDR continuously monitors dozens of IT and OT networks. Thanks to a combination of dual-level AI and advanced detection engines, it identifies suspicious activity often missed out by traditional security solutions. As cyberattacks evolve, proactive monitoring of network traffic via an NDR becomes a vital necessity to protect digital assets. »

Identity fraud techniques are evolving rapidly

Sara Sebti
CEO and co-founder

« In 2024, cybercriminals are increasingly targeting digital identity. We are seeing an uptick in deepfakes, and fraud techniques powered by artificial intelligence to steal identities and bypass traditional security systems. While these threats represent a major danger to digital confidence, they can also have a significant impact on the online economy. It is therefore essential to put in place strong authentication solutions and constantly innovate to combat the new fraud techniques used, even the most sophisticated ones. Artificial intelligence combined with biometrics can play a crucial role in this fight. »

When a QR code opens a Pandora's box to cyber attacks

Nathalie Launay
Senior Expert Consultant in Digital Identity at Galitt, a subsidiary of Sopra Steria

« COVID has accelerated the adoption of QR codes for contactless proximity interaction (ordering at a restaurant table, etc.). With smartphones, its use is spreading rapidly, including online. However, this visual code is becoming a Trojan horse for payment fraud (QR code to pay for electricity recharging, etc.), for stealing authentication data (receipt from the Post Office in your letterbox or «phishing» by email), or even for installing spyware. In addition to a trusted app for scanning, the new standards and wallets for instant payment or digital identity (EUDIW) require the adoption of interoperable secure codes, such as the Visible Electronic Stamp developed in France, adopted by the ANTS, and standardised (Afnor and ISO). »

The increase in hybrid attacks

Mickaël Wajnglas
General secretary

« There is a clear trend towards an increase in hybrid attacks. This means that an attacker can first physically break into a building, and then more easily reach the heart of the information system to carry out a cyber-attack. There are many different hybrid attacks, including attacks targeting security hardware devices perimeter such as access control readers or video protection cameras. The EU has taken full account of this new challenge with the NIS 2 Directive, which for the first time combines physical and cybersecurity. SPAC Alliance is proud to stand alongside ACN in providing its security expertise and raising awareness of these new threats throughout the market. »

Our 2024 forecasts: one step closer to the cyber end of the world?

Vincent Nguyen
Cybersecurity Director

« In 2024, attacks exploiting known vulnerabilities and supply chains, particularly Cloud services, will predominate. Advances in AI and IoT, while not currently disruptive, require increased surveillance. Security will be crucial during the Paris 2024 Games. NIS 2 is revolutionising compliance by imposing strict security standards on many organisations. Cyber insurance is becoming essential, offering financial protection and regulatory compliance. Organisations need to improve their defences, refine their incident response, and check the adequacy of their insurance cover. In 2024, anticipating threats and adapting quickly will be vital to navigating a complex and risky cyber environment. »

The resurgence of cyberattacks

Yannick Ragonneau
Associate Director

« The approach of the 2024 Olympic Games is causing a growing concern about the resurgence of cyberattacks. With an exponential increase in the attack surface and a multiplication of targets, no sector is spared. Traditional attacks are being revisited thanks to AI, as in the case of the president scam, which is already benefiting from the sophistication of deepfakes. Faced with this threat, it is becoming urgent and strategic to change the paradigm and move from a reactive to a proactive «resilient» approach. The organisation of the 2024 Olympic Games should be seen as an opportunity to transform our technological services so that they can learn to react to and withstand geopolitical tensions, cyberattacks and the changes brought about by digital acceleration. »

Patrick Bas
CNRS researcher

Teddy Furon
INRIA researcher

On the need to legislate on the design of AI-based content generators

« AI-generated content is becoming increasingly realistic. Passive forensic analysis methods provide only a temporary solution, given the need to update detectors and the potential difficulty of the task. Active protection consists of using a watermarking system to modify contents in an imperceptible way, while embedding a message to prove that the content has been generated. This type of method can only be deployed if there is legislation requiring generator suppliers to incorporate the watermark. The solution also needs to be robust to normal processing and to hostile attacks. The French scientific community is well positioned to meet this challenge. »

Focus - SPAC

MARKET TREND: INCREASE IN HYBRID ATTACKS

Mickaël Wajnglas
General Secretary SPAC Alliance

The increase in cyberattacks is nothing new. This trend has been observed for many years. What is rather new is the trend towards an increase in hybrid attacks.

1. What is a hybrid attack?

The objective of a cyberattack and a hybrid attack is the same - to attack or penetrate the information system (IS) for malicious purposes. Whereas a cyberattack is carried out remotely, using vulnerabilities in the IS, a hybrid attack uses physical means. To put it plainly, in a hybrid attack, an attacker will first physically break into a building, to then more easily reach the heart of the IS and complete his cyberattack.

It should be noted that the reverse process also exists. In this case, the cyberattack is carried out upstream, to gain access to and control the IS, and then facilitate a physical intrusion.

2. What are the different types of hybrid attack?

There are two main families of hybrid attacks: those that exploit the human factor, and those that exploit security and cybersecurity flaws in the ecosystem of connected devices.

In an attack exploiting the human factor, the attacker's objective is to break into an organisation's infrastructure by any means possible, for example by bribing or luring security staff at the entrance to the building.

In the case of a USB key attack, the attacker will not try to penetrate the building himself, but will use the curiosity and potential credulity of staff with little awareness of cybersecurity issues. For example, the process might involve leaving one or more USB sticks containing malware in a company car park. This key is then retrieved by an employee, who physically introduces the corrupted device into the building and connects it to their computer, which is itself connected to the network.

The Stuxnet worm that destabilised Iran's nuclear programme is a perfect example of this type of attack.

There are also many examples of attacks targeting perimeter or IoT security equipment, such as the connection to a camera on an unsecured IP network. As far as access control is concerned, if the reader or the communication protocol does not offer the highest levels of security, there is a risk that an attacker will carry out a reader substitution in order to recover the secrets (encryption keys). Replay

attacks are also possible if the communication protocol between the access reader and the IS does not offer the highest levels of security. An attacker could eavesdrop/intercept communications.

It should also be borne in mind that around 70% of access badges still incorporate obsolete technologies. An attacker can therefore very easily and very quickly clone an employee's access badge to gain entry to the building and then access the network.

3. The consequences of a hybrid attack

«When you lose control of a place, you have to assume that everything is compromised» NIST
This quote from the US federal agency following the assault on the Capitol perfectly sums up the impact that a hybrid attack can have on an organisation.

We all know that hundreds of people stormed the Capitol in 2021 for what was originally an insurrectionary purpose. This attack led to numerous acts of vandalism and ransacking. What is less well known, however, is that a large amount of computer equipment containing secrets, critical information and access data was stolen.

It is highly likely that it was not just supporters unhappy with the outcome of the US presidential election who took part in this assault. There is a good chance that many of the computer peripherals left behind were also infected. It's easy to imagine the consequences and impact this event has had on the country in terms of cybersecurity and national security.

Today, we know that after this event, an increase in intrusion attempts on the networks of US administrations was identified.

Given the scale of this hybrid attack, the incident response process put in place was much more complex than if the Capitol had been confronted with a «classic» cyberattack.

Even today, any cyber risk linked to this hybrid attack cannot be 100% ruled out...

4. Cybersecurity and physical security, a European paradigm shift

The evolution of threats, particularly the increase in hybrid attacks, means that we now must consider cybersecurity as intimately linked to physical security. An organisation can be equipped with the highest levels of cyber protection, but if the front door of the building is left open, the information system will be even more exposed.
The European Union has fully taken on board this new challenge: the NIS 2 Directive, which will come into force in October 2024, makes a clear and explicit link between cybersecurity and safety for the first time.

Physical and logical security now go hand in hand.

5. Countermeasures

The challenge of protecting all physical security solutions is a major one.

First, because physical security is now seen as the first line of defence against unauthorised access to an organisation's IS. Secondly, because these security devices are generally installed at the perimeter of buildings, i.e. in unsecured areas, due to their business application.

What's more, the deployment of IoT devices is increasing rapidly, thanks to the rise of the Smart Building. Even though these connected objects are generally installed in secured areas (inside the building), most of them have very little security. This increases the attack surface of the building. That's why it's so important to integrate sovereign, standard European technologies, and protocols with the highest levels of security, such as SSCP®. Hence the importance of integrating sovereign, standard European technologies, and protocols with the highest levels of security, such as SSCP®. This communication protocol, historically designed for access control, is the only one to have received CSPN certification from ANSSI, and it is now the most widely integrated protocol in certified access control solutions on the market.

This protocol was opened in 2020 through the SPAC Alliance to become the only European industry standard enabling access control devices to communicate with the IS.

Standardisation has also opened this protocol to other security ecosystems, such as intrusion and video protection. The aim, once again, is to offer the highest levels of security, but also and above all uniform levels of security throughout the physical security ecosystem.

V

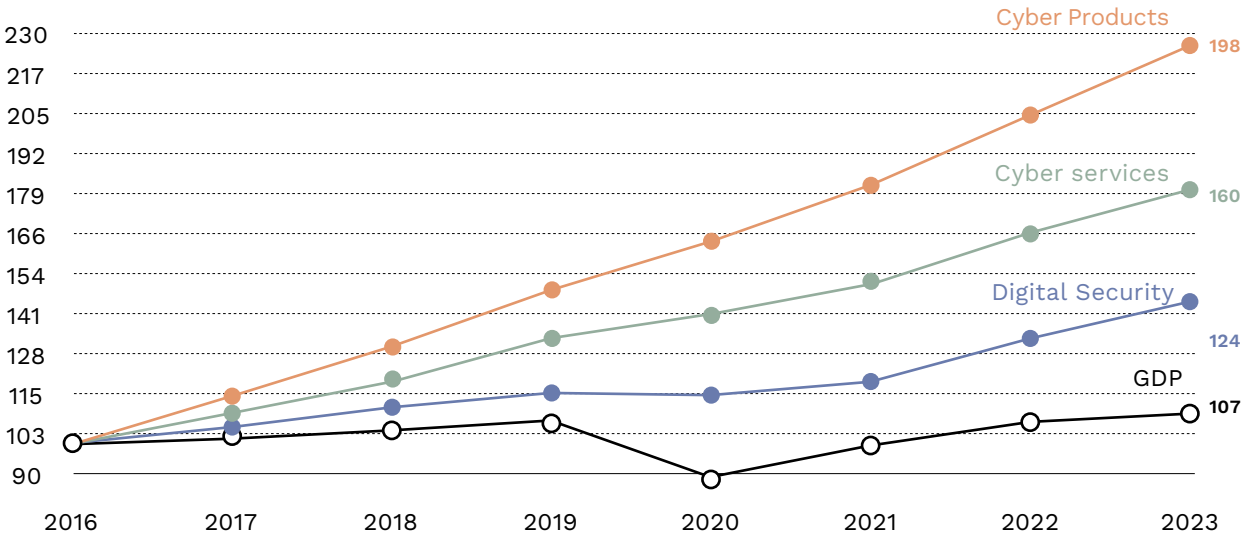
MARKET TRENDS

V. MARKET TRENDS

5.1 General trends

The graph below shows the comparative growth of the three main segments of the Digital Trust industry and GDP over the 2016-2022 period.

France growth comparison 2017-2023



	Growth					
Segments	**2018**	**2019**	**2020**	**2021**	**2022**	**2023**
Digital Trust	**8,2 %**	**8,5 %**	**3,6 %**	**7,3 %**	**11,3 %**	**9,6 %**
Cyber Products	13,9 %	14,0 %	10,9 %	8,8 %	12,6 %	11,1 %
Cyber Services	9,9 %	10,3 %	5,8 %	8,9 %	10,3 %	8,6 %
Digital Security	4,7 %	4,8 %	-1,7 %	5,2 %	11 %	8,9 %
GDP	1,9 %	1,8 %	-7,8 %	6,8 %	2,5 %	0,9 %

Source : INSEE

5.1.a. The growth of the French sector

Particularly strong growth in 2022, continuing into 2023

2022 is marked by a particularly strong growth. Cybersecurity had an excellent year, with growth of 11.5%, in line with the 2014-2019 trend. However, digital security had an exceptional year, with growth of 11%. This growth was driven in particular by market leaders Thales, Airbus (worldwide), IN Groupe and IDEMIA, through projects linked to access control and identification. This is the case for IDEMIA, for example, through several partnerships launched since 2021 (central border control system in partnership with the French Ministry of the Interior, reinforcement of its multi-biometric identification system with INTERPOL, contribution to the France Identité Numérique program and to the "digital identity guarantee service" with the Agence nationale des titres sécurisés). But this growth in digital security was also supported by an increase in exports, notably to Europe, but also worldwide.

At the same time, other explanatory factors remain:

■ A rebound effect following the period of recession associated with the COVID crisis (nearly -2% in 2020, with some major players experiencing a recession until 2021).

■ The impact of higher semiconductor prices following the global shortage, leading to growth in value. This is particularly true for the personal identification and authentication segment (smart cards, etc.) and for the cyber segment of equipment security (secure components, HSM), but this phenomenon extends to the whole of digital security.

■ Finally, a favorable economic climate is driving growth in volume: the growing importance of border control, with public projects on the rise, increased demand for security from European states in the wake of the war in Ukraine, and the securing of major events (Rugby World Cup in France in 2023, Paris Olympics in 2024, etc.).

Although less exceptional than 2022, 2023 remains a year of strong growth for digital trust, with growth of 9.6% overall, i.e. 8.9% in digital security and 10.1% in cybersecurity.

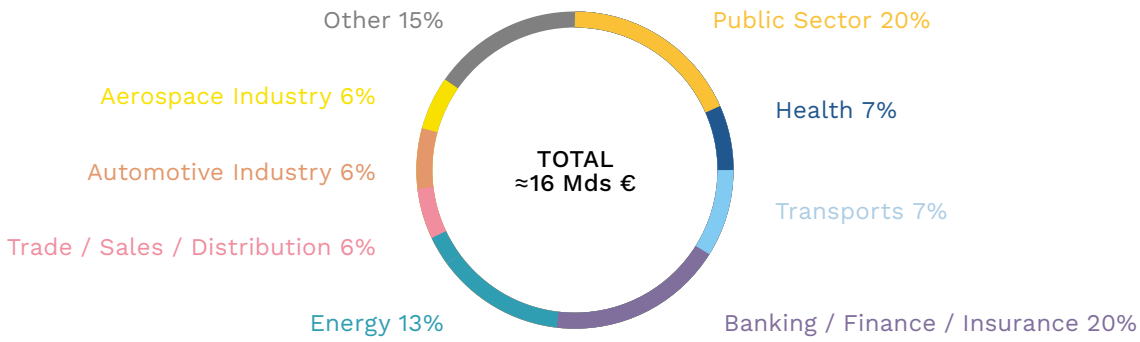
The industry's leaders continue to grow: Thales and Airbus reported lower organic growth of between 2% and 5% in their digital trust activities, while Idemia and IN Groupe maintained their momentum with double-digit growth in their digital trust activities. Cybersecurity is also continuing its past trends, with leaders such as Docaposte and Sopra Steria (the latter, for example, is involved with IDEMIA in the FAED V3 project to modernize the fingerprint management system) recording growth of between 10 and 15% over 2023.

5.1.b. Markets in the industry

As shown in the diagram, the **public sector** in the broadest sense, i.e. including transport and healthcare, **accounts for a third of the French market** (€6 billion in 2023), with the remaining two-thirds coming from the private sector (€11-12 billion).

The weight of the private sector is set to grow year on year. The Digital Trust sector originated with the French government and the need to secure its Vital Information Operators (VIOs). The need for trust then spread to large companies in general, beyond the OIVs. The current trend is to develop the market for SMEs and VSEs, most of which are now helpless in the face of the risk of cyber-attacks, particularly ransomware.

Main Markets for the industry in 2023



Source: DECISION Etudes & Conseil, form filled in by companies in the industry

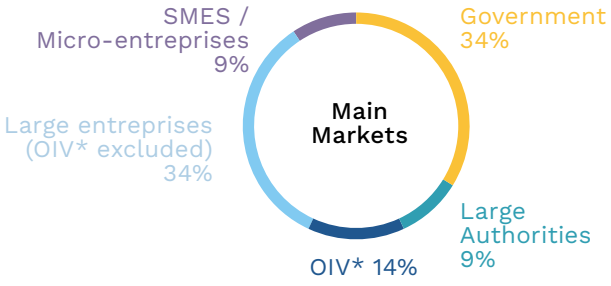
For the year 2023, however, the public sector continues to be indicated as one of the main growth drivers by the companies in the sector who responded to our questionnaire, alongside the Banking / Finance / Insurance and Energy sectors.

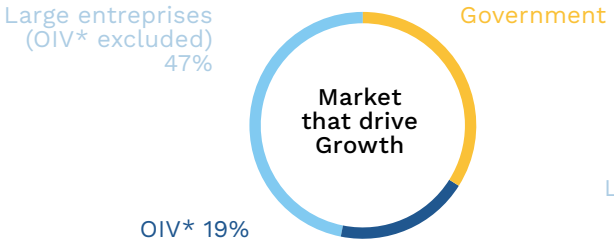
The emergence of a market for Micro-entreprise/SMEs and small local authorities

The following series of diagrams, taken from the 2024 edition of the online survey of industry players, shows the segmentation of the French industry market according to the type of company supplying trust solutions (large-scale enterprise versus micro-enterprises / SMEs).

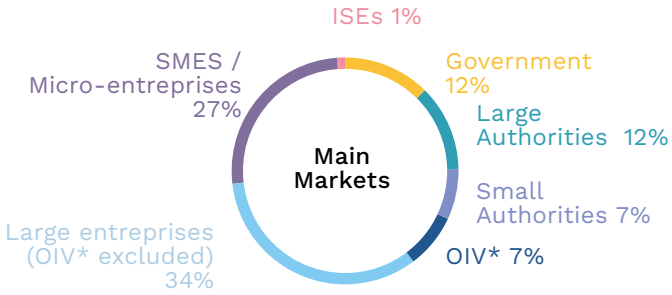
It can be seen that the French government, Opérateurs d'Importance Vitale (OIV) and large companies (excluding OIV) account for over 80% of the market for large companies in the sector, and nearly 100% of their growth prospects for the coming years. These large-scale suppliers of trust solutions will account for 54% of the industry's sales in France in 2023 (72% if activities outside France are included). Here, we find the traditional markets around which the industry was built: the French government, OIVs and major private accounts.

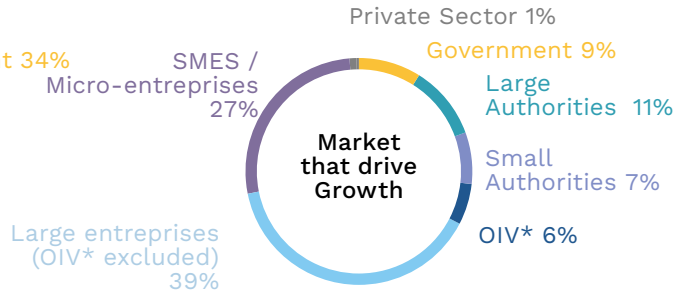
Large entreprises





Micro-entreprises / SMEs





* Opérateur d'Importance Vitale = Vital Importance Operator

In contrast, the State and the OIV only represent 20% of the market for SMEs and Micro-entreprises in the sector. Large enterprises (33%), Micro-entreprise/SMEs (26%) and local authorities (20%) account for the bulk of the market and growth prospects for SMEs and Micro-entreprises providing trust solutions in France. In other words, through this vision of SMEs and Micro-entreprises in the sector, we can see the emergence of two markets:

■ **That of local authorities,** including small local authorities. By extrapolation, the market for small local authorities can be estimated at between €1 billion and €1.5 billion in 2023.

■ But most of all, **the development of the market associated with the need for trusted products and services from French SMEs and Micro-entreprises.** By extrapolation, this market can be estimated at between 2.6 and 3.6 billion euros in 2023. This market is characterized by dedicated offers: standardized offer, rapid deployment, low cost, often without hardware support, etc.

The development of this market for French SMEs and Micro-entreprises was slowed down in 2020 by the COVID crisis. Indeed, French SMEs and Micro-entreprises were more affected by the restrictions associated with COVID than the traditional large customers of the Digital Trust sector (State, IGOs, large companies), which are particularly focused on the supply of essential needs (Banking/Finance/Insurance, Energy, Health, etc.)

However, the structural trend is indeed towards the development of this SME and Micro-entreprise market, which is destined to become one of the major markets of the sector and will underpin its growth in the years to come.

5.1.c A major workforce shortage that can be overcome

The gap between workforce requirements and the number of available professionals is widening, despite an increase in the number of people trained in cybersecurity. Faced with a growing threat and a rapidly evolving technological landscape, the sector has been confronted with budget cuts due to the economic climate. Yet information security is increasingly at risk during these uncertain economic times.

In its 2023 survey of cybersecurity professions, ANSSI suggests three main areas to tackle to mitigate the shortage of cybersecurity talent:

■ Work on the image of the cybersecurity sector to make it more attractive. ANSSI points to a lack of understanding of the realities of the profession among students, and suggests demystifying the sector while promoting enhanced education in digital uses from an early age. This includes diversifying representations of the sector to attract a wider range of talent, and developing a culture of cybersecurity in society.

■ Democratize access to cybersecurity careers by diversifying profiles and career paths. The report criticizes the elitist, highly technical image of the sector, which deters many potential candidates. To this end, it suggests broadening the profiles recruited, promoting professional retraining and non-traditional skills, and clarifying training paths and career development opportunities.

■ Improving working conditions in the cybersecurity sector. The report notes that only 63% of professionals feel socially valued in their profession, and that in the private sector in particular, a cyber culture needs to be developed to make cybersecurity a strategic issue recognized by all. This also requires better remuneration and more attractive contracts to retain talent in a field where skills are scarce and precious.

In March 2023, ANSSI published a survey on the attractiveness of the cybersecurity sector

Survey 2023
'The attractiveness and representation of cybersecurity professions'

Focus - Ecole 2600

THE «SKILLS FIRST» APPROACH TO INCREASING SKILLS AND RESPONDING TO LABOUR SHORTAGES IN THE SECTOR

Valérie Poulain de Saint-Père
President and co-founder of Ecole 2600

2023 was a gloomy year for cybersecurity: while the number of successful cyberattacks remained stable, according to the CESIN (Club des Experts de la Sécurité de l'Information et du Numérique --Information and digital security Expert Club) barometer almost half of French businesses were attacked. Figures recently published by the ANSSI (Agence nationale de la sécurité des systèmes d'information) confirm it: acts of cybercrime in our country have increased by 400% between 2020 and 2023! Not only is the threat still omnipresent, but it also has a dangerous capacity to reinvent itself.

Against this worrying backdrop of digital warfare and the professionalisation of cybercriminals, and at a time when 68% of business leaders are making protection against cyberthreats their top priority for 2024, according to a survey by BDO, it is up to the cybersecurity training providers themselves to embrace this ability to reinvent themselves: while massively accelerating training, to train more cybercrime experts, it is imperative to change the paradigm to train them better.

We are convinced that the 'skills first' approach will facilitate the emergence of 'new collars', along the lines of IBM's P-Tech project.) This new culture, based on skills, will lead to greater internal mobility, a reduction in the attrition rate of employees and, above all, a culture that favours skills over diplomas alone. This would make it possible to fill vacant positions, develop talent that is often overlooked and promote socio-economic diversity.

This paradigm shift is set to take shape in a new assessment model. Better adapted to the concrete needs of businesses, it would replace the current over-emphasis on generic diplomas with the hy personalisation of continuing education, through the certification of micro-skills in cybersecurity. This is the whole purpose of the 'lifelong' training platform that we have deployed at École 2600.

We started from a very simple postulate: to guarantee the highest level of performance from experts in the face of the technological developments from which cybercriminals benefit (machine learning, generative artificial intelligence,

quantum algorithms, etc.), their skills need to be regularly reassessed and updated. They must also correspond to specific modules, to achieve the finest possible level of granularity.

The emergence of this new model of continuing education based on micro-certification will enable us to build up a pool of experts with maximum agility, adaptability, and speed, close to companies and institutions. Many companies are not yet able to assess the skills of their employees, and hence the risks and skills that need to be developed to anticipate them.

At a time when the French cybersecurity market is in short supply, with 15,000 vacancies compared with the 37,000 jobs needed between now and 2035, this new training model will also make it possible to up-skill and/or re-skill a company's employees, to guarantee the continuity of cyber expertise within the company.

To ensure that our platform is as effective as possible, we believe it is essential to back it up with a pragmatic two-pronged approach.

First, dealing with a global threat requires a global approach. That's why the platform is aligned with the European Union's strategic guidelines on the development of a European skills repository. We have created job descriptions for each profession, with skills that include ENISA's reference frameworks as well as NIST's NICE and ANSSI's, in addition to our own reference framework.

Finally, to ensure the finest possible link between the training courses on offer and the real needs of companies, it is essential to map the latter. This is the purpose of the skills collection and extraction tool and the mapping of technical stacks that we have put in place, to monitor in real time the state of skills requirements worldwide in relation to advertised job vacancies.

Faced with all these major challenges and the growing threat of cyber-attacks, École 2600 will continue to defend a relevant and powerful cybersecurity training model, capable of contributing to the imperative need for a sovereign and solid national cyberdefence, in the interests of our companies and our country.

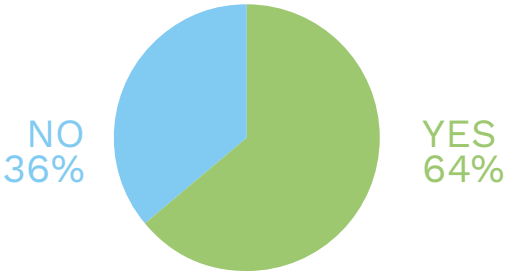
Zoom - Ecological transition in the sector

At a time when the ecological transition is a priority for everyone, each sector is considering the best way to act in the light of its challenges and constraints. ACN has initiated a wide-ranging debate on this issue to enable companies in the sector to share their best practices and pool their thoughts to position our sector on an ambitious trajectory of ecological transition.

As part of this 2024 edition of the ACN Observatory of Digital Trust, we wanted to shed some quantitative and qualitative light on the reality of this transition in our sector. To this end, we questioned digital trust manufacturers about their involvement and their motivation to implement actions to reduce their environmental footprint.

2/3 of companies surveyed consider the ecological transition to be a priority.

Is the ecological transition a priority for your company?



Ecological transistion: a major issue for the industry

2% of sales

this is the estimated amount invested by companies in the sector in ecological transition initiatives.

Actions already taken

Most companies in the sector are aware of the need to take action to limit the carbon footprint of their activities.

To reduce their footprint, we wanted to know whether they are focusing on actions to optimise their consumption of resources in their processes (design, deployment, operation) or whether they are implementing strategies to offset their direct impact.

Today, are the actions you take to limit the carbon impact of your products services/technologies?

41% Actions to reduce their consumption of resources at source (design, deployment operation)

0% Remedial action to offset their direct impact

41% A bit of both

18% In any case, we are still too far removed from these issues. or improving safety remain our top priorities.

Two types of action were highlighted: 41% of companies are optimising their resource consumption and 41% are optimising their resource consumption and at the same time offsetting their direct impact.

The offsetting lever is never used on its own, and that only 18% of the companies surveyed have chosen not to take any action.

Companies' motivations for taking action

When we asked them about their motivations for acting in this area, the companies in the sector ranked their priorities in the following order:

As a company director, what are/should be your motivations for to make (or not to make) a commitment to ecological transition?

1. Improve your technological performance to enable new uses
2. Comply with current legal requirements and standards
3. Reduce your operating costs through more sustainable practices
4. Use the ecological transition as a marketing argument to attract customers
5. Strengthen your employer brand through your commitment to the environment
6. Ensure technological leadership for the future
7. None of the above; you have other more pressing priorities linked to your core business

It should be noted that motivation linked to the marketing use of these actions only comes in fourth place, indicating a deep understanding of ecological issues on the part of companies.

Chantal Droulez sheds light on the ecological transition

Chantal Droulez

President of AwaCloud and Chair of the CSF Industries and Security ecological transition working group

In your opinion, what are the major challenges of the ecological transition in the digital trust sector?

The objective of reducing greenhouse gases is estimated at -30% by 2030. The current consensus is that the optimisation measures envisaged will not enable us to achieve this target because they will be immediately consumed by the growth in usage. Additional measures will therefore be needed to develop energy efficiency. In this respect, one of the challenges is to evolve software development practices to produce tools that are more frugal in their consumption of resources and more modular in their design, to deliver to customers only those services that are useful to them. This will necessarily involve changing the practices and skills of both developers and architects. It is also important to understand that, like security by design, green by design implies more radical choices and, consequently, more restrictive technical requirements, resulting in longer development times. This raises the question of acceleration mechanisms, given the scale of the changes to be made.

What is being done to help businesses make the ecological transition?

There are too many initiatives to list exhaustively. Among the many initiatives, I would highlight Numeum's Planet Tech'Care initiative, which mobilises their network of partners to reduce the environmental impact of digital technology. Campus Cyber's Cyber4tomorrow initiative aims to integrate and disseminate the principles of sustainable development in the cybersecurity sector and, of course, The Shift Project, which is leading several discussions on digital sobriety. These various initiatives should be seen in the context of Cigref's initiatives to raise awareness and disseminate best practice among CIOs and CISOs.

At the level of the digital trust sector, ACN has undertaken to mobilise companies in the sector, to measure their activity in terms of ecological transition (notably through their 2024 Digital Trust Observatory) and to lead their discussions in internal working groups to encourage the pooling and sharing of best practices. Lastly, the Strategic Sector Committees (SSCs) all include a section on ecological transition in their sector contracts. The Security Industries CSF has a dedicated working group, in which ACN plays an active part. There is a lot to be done, and the sector is gearing up to move forward.

What are the most promising ways of reducing greenhouse gases in the digital sector?

The first (and most obvious) route is software optimisation. The technologies developed in recent years have been developed without resource constraints and are generally not very optimised from a code point of view.

Advantage: the potential for optimisation is there.

Difficulty: In a context where there is a race for additional functionalities and a shortage of developers, dedicating resources to optimising code is a difficult decision, if not impossible because of the intertwining of software dependencies. The paradox is that the more integrated the software, the greater the potential for optimisation and the less accessible it is. This reduces the scope of this lever. Those most likely to be able to mobilise it with significant results are those who have complete control over their technological supply chain or who have a weak legacy.

Another approach is the functionality economy. This involves a very detailed analysis of the needs we wish to address and radical choices in terms of architecture. The results can be impressive. One American company, for example, recently reported cloud resource savings of over 98%. To mobilise this leverage on existing products, you would have to agree to completely redesign them. So, it's more likely to be start-ups that are investing in this field.

There is also the option of modular architectures designed to deliver only the services the customer needs. In the long term, this is probably one of the most important levers, particularly if we combine it with the previous one, with the emergence of a digital world that is very different from the one we know today. But on these issues, we are still in the early stages.

To conclude, the ecological transition is today a tremendous opportunity for digital development. And because of the nature of the changes that need to be made, it is also a fantastic opportunity to integrate security issues at source. ”

Focus - AN2V

DIGITAL TRUST ... TERRITORIES: 34,935 MUNICIPALITIES TO SUPPORT !

Dominique Legrand

President and co-founder of AN2V

How to help (all) mayors, especially those in rural areas, to set up a video protection system linked to a monitoring centre 24 hours a day, 365 days a year, with a direct link to the gendarmerie.

In rural areas, the current operation of video protection systems, where they exist, is designed to meet several different goals, such as personal safety, helping people (removing doubts, understanding a public site against fire and accidents, unusual gatherings, etc.), preventing damages to property, preventing acts of terrorism, and so on.

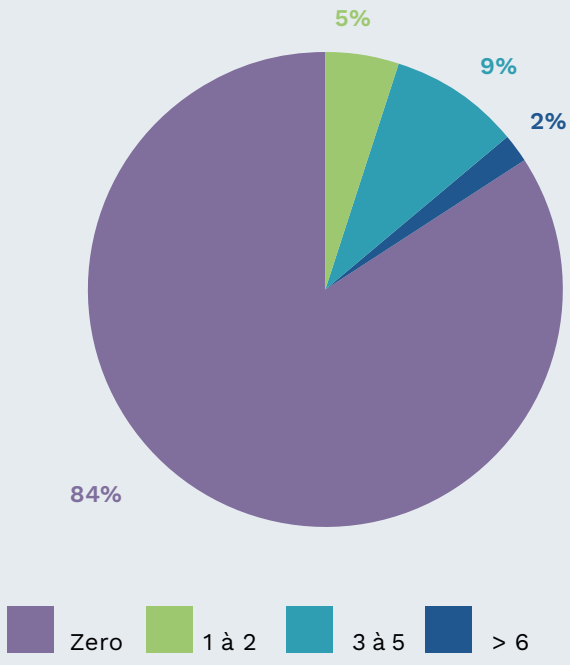
All you have to do is carry out a survey of one of the 101 French departments to observe the equipment and functioning of municipalities with fewer than 2,000 or 5,000 inhabitants, and you will understand that as soon as you move away from the prefectures and sub-prefectures that have a real Urban Supervision Centre (CSU) and a solid IT department, the small municipalities can unfortunately only do their best: purchasing 3 to 10 inexpensive Asian cameras, some of which are stand-alone and have no optical fiber connection (so they are recorded locally), and some of which have a 4G/5G radio link (40%), but this is often not maintained centrally at the town hall, and there is no active CSU; there is no operator, so there is no 24-hour service Finally, when it comes to the GDPR and the cyber risk for these systems, there is little or no expertise in this area. It is common knowledge that the video protection system is often the weakest link enabling a hacker to gain access to a town hall's entire IT system! And even though it is often claimed that the video system is isolated and «quite separated», a quick analysis will quickly reveal IP links with the town hall's other networks, for reasons of maintenance, updating servers, sharing data on certain applications, etc.

It is therefore worth considering a major overhaul of all these systems to smoothly integrate new uses (smart and sustainable), and to best meet the new service expectations of all our fellow citizens.

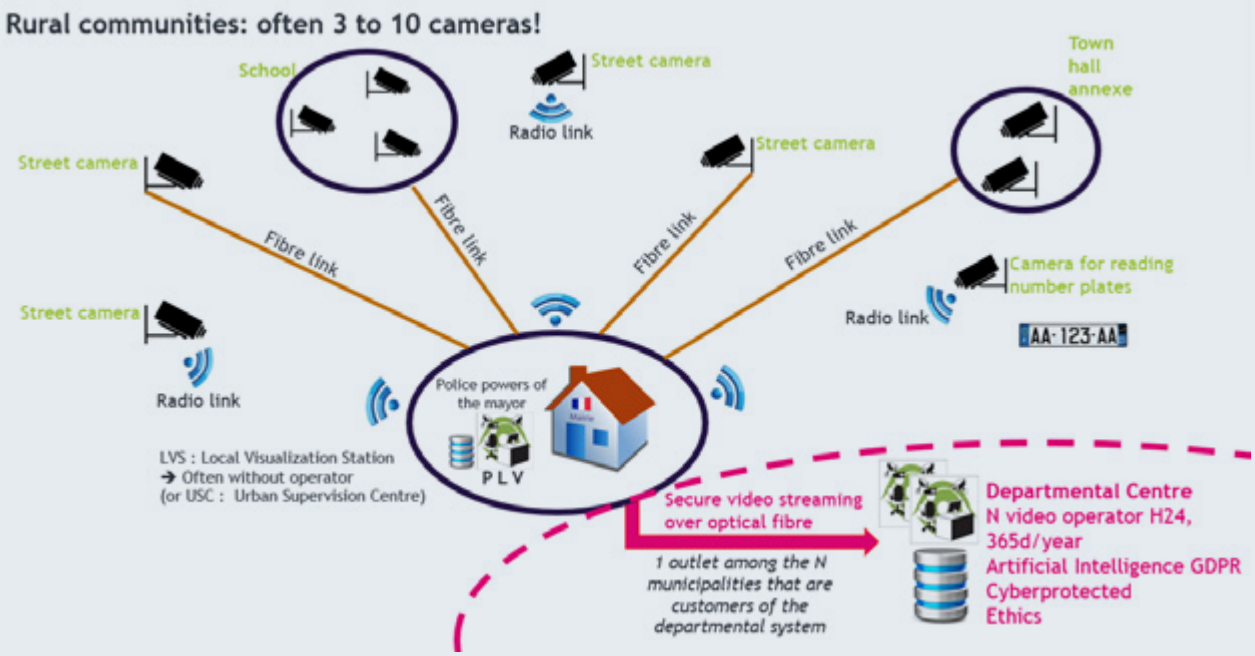
In all French departments, a fibre-optic broadband network has been rolled out to all municipalities, and if this has not yet been done, it will be soon, within a few years, with the abandonment of copper at the subscriber's premises (Plan France Très Haut Débit launched in 2013).

Local authorities want to integrate new uses and study the automatic detection methods provided by image analysis (Artificial Intelligence), the interpretation of events from other sensors (trusted IoT) or external applications (on citizens' smartphones).

This is now possible under Article 42 of the Comprehensive Security Act, which safeguards freedoms (Article L132-14 of the Interior Security Code - version in force since 27 May 2021, amended by Act no. 2021-646 of 25 May 2021 - Article 42). Pooling video protection systems across a department is an undeniable source of efficiency: from an operational point of view, it makes it possible to achieve the critical mass needed to set up a supervisory centre staffed by video operators which process images in real time 24 hours a day, 365 days a year, as well as providing high-performance new-generation tools (AI, rapid searches, etc.). It also means that the green and orange zones in the pie chart above (i.e. 89% of municipalities) can be covered in a single operation. It also means that a larger, more coherent area can be covered, on the scale of a catchment area, as mentioned in the 2018 parliamentary report on the security continuum by Alice Thourot and Jean-Michel Fauvergue. Inter-communal cooperation was already provided by the internal security code, so there was no need to legislate on the subject, but this pooling of video protection systems only concerns municipalities within a communal block. The most rural communes were never able to reach a volume justifying the creation of an operating post, even within their community of communes.



CSU: The number of operators dedicated to video protection systems in public spaces is striking: An analysis of the municipalities in a department with more than one million inhabitants located in the Paris suburbs gives the following result: the systems are overwhelmingly «passive», with no operator in 84% of cases. Only the 10 largest towns have such systems, representing 2%!



AN2V has therefore long been denouncing this safety divide between rural or semi-rural areas and towns and city centres.

Since 2021, this law has provided a very attractive solution for rural municipalities. To date, some fifteen departments, through their mixed digital syndicates, have embarked on studies on this subject, and in April 2024, 5 departments were already equipped!

ACN and AN2V are joining forces to make this type of project a reality, because the technical and organisational challenges are numerous! In fact, it is essential to have a firm grasp of:

- The areas of technical and legal responsibility between the client local authorities and the central system provider (e.g. the SMN - Syndicat Mixte Numérique), with agreements to be drawn up! Formal relations need to be established with the FSI - Forces de Sécurité Intérieure...

- A transparent definition of the organisation of the project, the «who does what when»! The training of central video operators, their day and night mission sheets...

- The IP interconnection network with the client municipality's video protection networks, its actual architecture (which may need to be reviewed, IP addressing, QoS, etc.),

- The IT architecture for shared storage (locally on site and/or with a host), with possible redundancy at the central office and at the local authority,

- A video stream management system capable of handling such a heavy load (VMS - video management software), thousands of video streams to be prioritised, etc.

- A shared, trusted AI software suite on safe, smart, and sustainable subjects, and more generally, a close relationship with the project's DPO/DPD to ensure that the data circulating is perfectly supervised within the meaning of the GDPR and respect for individual freedoms,

- Strong resistance to any type of cyberattack, and at the very least, strong compartmentalisation to avoid any domino effect.

5.2 Regulatory trends

5.2.a. European regulatory landscape: a trusted digital single market is emerging

Digital transformation continues its journey within the EU. The new risks arising from new uses are prompting the European institutions and the Member States to consider ways of adapting our legislative arsenal to these developments and enabling the European Union to take control of its digital future. The «Digital Europe» programme, through which this response is taking place, aims to make Europe a major player in this field, to strengthen its technological sovereignty and to ensure its resilience in a context of growing tension in cyberspace. This year, many European draft texts are continuing their legislative journey and are on the verge of coming to fruition. These projects concern cybersecurity, and more specifically the strengthening of resilience, digital identity, market regulation and the establishment of a legal framework for artificial intelligence.

All of this work is a priority for the digital trust industry. 2024 is a pivotal year from an institutional point of view in Europe, marked by the renewal of the European Parliament and Commission. In the run-up to these elections, in April 2024 ACN published its European priorities and recommendations to accelerate the transition toward a single digital trusted market.

Strengthening cybersecurity

The Cyber Resilience Act (CRA) draft, which aims at establishing common cybersecurity requirements for products with digital components, is continuing its legislative progress. Prior to its adoption by the European Parliament in March 2024, a few amendments have been made to the text, to bring its provisions into line with the existing legislation (NIS 2 Directive, Cybersecurity Act, etc.). To date, the EU Council has yet to adopt the draft regulation. In the face of growing cyber security risks, the Cyber Solidarity Act has also been used as a legislative tool to strengthen European solidarity in this area, with the aim of setting up a European Cyber Shield, a Cyber Emergency Mechanism which would create European Cyber Reserve, and a Cyber Incident Analysis Mechanism. After a trialogue that reduced the original budget allocated to the European Cyber Reserve, the text still must be adopted by the European Council, as the Parliament has already voted on it on March 2024.

ACN Documentation
“2024 European priorities for the digital trust industry”

Available on the following link:
www.confiance-numerique.fr

Finally, after prolific legislative exercise on the beginning of 2023, the Member States now have several texts to transpose into their national law. The NIS 2 Directive, the Directive on the Resilience of Critical Entities (RCE Directive) and the requirements of the DORA Regulation must be implemented between the end of 2024 and the beginning of 2025.

Implementing an interoperable European digital identity

Revising Works on the eIDAS regulation to implement a secure and interoperable digital identity in Europe have been achieved with its publication in the EU Official Journal. Europe is then on the verge of providing all its citizens with a personal digital wallet usable throughout its soil. It will be implemented based on common technical standards (Architecture and Reference Framework - ARF), which are still under discussion. By 2027, the Member States will have to provide every European citizen with a free digital identity wallet.

Applying digital market regulation

The Digital Service Act (DSA) and the Digital Market Act (DMA), which aim at protecting Europe's digital market from illegal content and products, as well as unfair practices by certain players, have both come into force. All the companies designated by these regulations have been identified to protect the European technological sovereignty.

The revision of the Liability for Defective Product Directive is also evolving to include cyber security vulnerabilities within its scope. The protection of users is thus further enhanced.

In addition, the European Commission is attempting to prepare the European Central Bank (ECB) for the introduction of a European public cryptocurrency through its «Digital Euro» proposal. The aim is to complement existing fiat money and private solutions. Discussions on this project are ongoing within the European institutions, particularly the ECB, also the launch of a digital euro is not guaranteed.

In addition to the **'Digital Identity Digital Identity'** documents, ACN has has developed a website to list and all French digital identity offerings. digital identity offerings.

To be found on the site:
https://identite.confiance-numerique.fr/

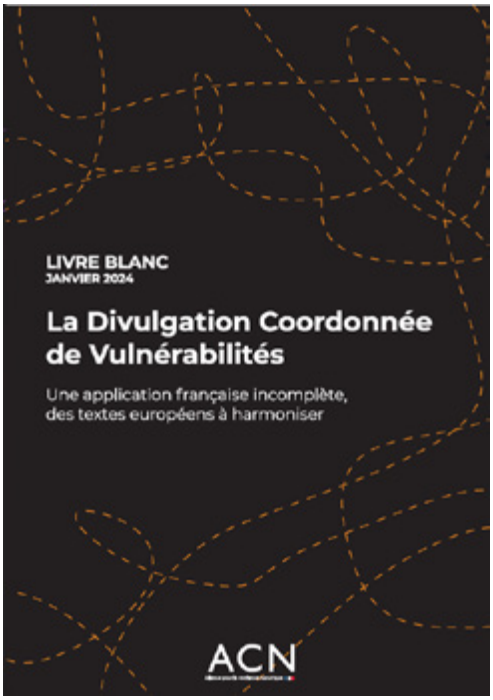
The creation of a European legal framework for artificial intelligence

The regulation on artificial intelligence (AI Act) was finally adopted by the Parliament and the Council of the EU at the beginning of 2024, after 3 years of negotiations. The prohibitions set out in the regulation will apply by the end of 2024, with a few exceptions for law enforcement agencies in the prevention of terrorist threats or in the search for targeted victims. Full implementation of this text, guided by the AI Office, which is already taking shape, is scheduled for 2026. The industry stresses the importance of this work. Indeed, the application of a European legal framework for AI is at the very essence of Trusted AI, which the industry has endeavoured to define through its white paper dedicated to Trusted AI.

Coordinated vulnerability disclosure: European momentum to build on :

The implementation of coordinated vulnerability disclosure policies has now been made mandatory by the NIS 2 Directive and the Cyber Resilience Act. The issue of discovering and dealing with vulnerabilities, which has been under discussion for several years, is regarded as central to the European approach to cyber security and as a major tool for increasing the level of protection and resilience of European entities. However, the initial responses put forward by the Member States of the European Union need to be standardised through a holistic approach. This would enable European legislation to be harmonised and would considerably reduce the legal uncertainty faced by many vulnerability researchers, especially in cross-border situations.

Conversely, the national legislation of each Member State could act as a spur. In France, several avenues are possible, such as revising the Penal Code to introduce an amendment that would protect bona fide vulnerability researchers from possible legal action by the seller. A national initiative of this kind could provide a major basis for drawing up the comprehensive legal framework that is currently lacking, thereby increasing the protection and resilience of our country and the European Union as a whole. In 2024, ACN published a white paper on the subject which compares the different European approaches and suggests ways of adapting our national legislation so that coordinated disclosure of vulnerabilities can make its full contribution to cybersecurity and resilience.



In March 2024, ACN published a white paper on the coordinated of Vulnerabilities

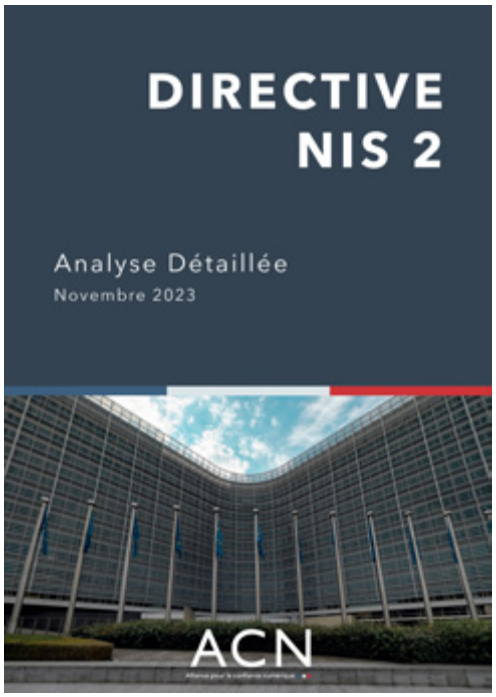
White Paper
'Coordinated Vulnerability of Vulnerabilities'
available for download on :
www.confiance-numerique.fr

5.2.b National digital trust initiatives

To meet the new challenges raised by the cyberspace evolutions and make France a worldwide player in cybersecurity, a national cybersecurity strategy has been rolled out since February 2021 by the President of the Republic. It makes the development of innovative, trusted, and sovereign solutions a priority. To this end, three waves of calls for projects were launched to support the securing of critical infrastructures, collaborative work suites, the resilience of the smallest structures and cybersecurity assessment. In the meantime, the national strategy for artificial intelligence (AI) is moving forward. A Generative AI Committee was launched in September 2023 which aims at informing the Government and making France a country at the forefront of the AI revolution.

France is also preparing for the entry in force of several European laws. Firstly, the "Securing and Regulating Digital Space" Act (Sécuriser et Réguler l'Espace Numérique - SREN) was definitively adopted by Parliament on 10 April 2024. Designed to adapt the national law to the European Digital Services Act (DSA) and Digital Markets Act (DMA), this text was proposed by the government in May 2023. In addition to the provisions required by these European texts, the SREN law includes several initiatives aiming at strengthening public order in the digital space and places digital trust at the heart of its project.

Lastly, a bill to transpose the NIS 2 Directive into French law is currently being drafted. The NIS 2 Directive provides that its requirements must be transposed into Member States' national law by October 17th, 2024. This bill will also transpose the directive on the resilience of critical entities (RCE) and the requirements of the regulation on the operational resilience (DORA) of financial entities.



ACN Report
«NIS 2 Directive Detailed Analysis»

Available at the following link:
www.confiance-numerique.fr

Focus - Strategic Sector Committees (SSC)

SHARED VIEWS OF THE STRATEGIC COMMITTEES OF THE SECURITY INDUSTRIES AND TRUSTED DIGITAL SOLUTIONS SECTORS

Marc Darmon

Chairman, CSF Security Indutries Strategic Committee

The security industry's strategic partnership with the French government was formally established ten years ago to meet the major industrial challenges of protecting the state, the economy and society. It was strengthened in 2018 with the creation of the Strategic Industry Committee (SIC), whose second industry contract (2024-2027) is due to be signed shortly.

What is the CSF's scope and field of action?

The Security Industries (SI) sector represents €32 billion and 157,000 jobs (2021). It brings together all the companies that provide technological security solutions and services (combating terrorism and serious crime, everyday security, personal rescue, border, infrastructure and network protection, cyber security, digital identification, etc.).

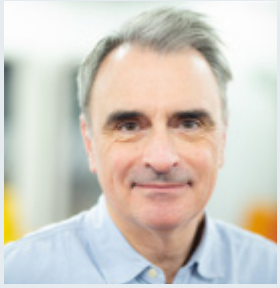
The new industry contract renews the vertical areas dealt with until now by the CSF IS (security of the Olympic Games and major events, cybersecurity, digital identity, trusted territories, and trusted digital technologies) and broadens its approach by introducing horizontal areas: competitiveness of SMEs, standardisation, international, mastery of technologies, attractiveness and skills, ecological transition, to activate more effectively all the levers for the development of the industry.

What are the main priorities that will be implemented within this framework?

The second contract is based on four priorities: growth of a competitive industry of excellence, mastery of key technologies of the future and critical technologies, attractiveness and skills, and support for the ecological transition. Its objectives are to intensify dialogue within the CSF with the French government, particularly on issues where the government's position determines solutions or influences the industry's business models, and to conduct ongoing strategic reflection on the industry's future and on new issues (trusted AI, the fight against information manipulation, etc.). In addition, this second contract aims to enable the industry to make progress towards high-quality, innovative, competitive, and ethical solutions, by stepping up dialogue with the markets. Finally, we are also giving priority to strengthening support for SMEs in the sector, links with research and the development of cross-functional initiatives to continue building a strong, sovereign industrial base.

What role would you like to see the ACN, and more broadly companies in the digital trust sector, play in your work?

ACN is a key player in the industry and has been a major contributor to its work and progress since its creation. It is at the heart of three key segments of the industry: digital identity, cybersecurity, and trusted AI. Through the technical work it carries out and its proactive and defensive actions in the areas of legislation, regulation, and standards, it is an essential link in the ecosystem and plays an irreplaceable role in the strategic dialogue with the State and with the European level. I hope that ACN will continue along this path with dynamism and help the industry to mobilise all the major levers at its disposal to achieve its key objectives.



Michel Paulin

Chairman, CSF Trusted Digital Solutions Strategic Committee

What is the CSF's scope and field of action?

The Trusted Digital Solutions sector encompasses software publishers and suppliers of digital tools, products, and services, excluding Digital services companies ("ESN") and consulting firms. With sales of €23.7 billion in 2023 and annual growth of 10%, it is one of the most dynamic sectors in the French industry. It is composed of players representing the key fields of cloud, artificial intelligence, quantum, immersive technologies, and software. The industry's Strategic Committee is the structure that brings together the French government and this ecosystem for a strategic dialogue on its development.

What are the main priorities that will be implemented within this framework?

The prefiguration mission of the Strategic Committee has identified 5 keys areas that will define its work over the next 3 years:

- Developing the offering and deploying the infrastructure needed for innovation (AI, etc.) in trusted digital services,

- Developing access to training and working with the government on innovation schemes to promote trusted digital technologies,

- Defining sensitive data and harmonising certifications and regulations,

- Facilitating access for trusted digital players to public and private sector procurement,

- International development of the sector.

What role would you like to see the ACN and, more broadly, companies in the digital trust sector play in your work?

Existing companies and organisations working in the digital trust sector play a major role in raising awareness, educating, putting people in touch with each other and boosting the Trusted Digital Solutions ecosystem. As such, we would like to include them in our working groups and invite them to join the Trusted Digital Solutions association to benefit from their expertise and their work on trusted digital technologies.

VI. 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.

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

b) The "Cloud au 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 first version of this cloud platform is scheduled for May 2024, and will include an expanding catalog of managed services.

3. Digital identities. Strongly correlated with the issue of data sovereignty, the need to redefine digital identities also stems from the development of electronic tools and digital transformation («remote citizenship»). The current norm in France remains the simultaneous existence of numerous uncorrelated identities, strong (SIM, bank cards, passports, etc.), substantial (La Poste's digital identity), and weak (digital identities issued mainly by American digital players such as GAFA for e-commerce), with no guarantee of sovereign data protection. The alternative is the deployment of an unique and sovereign strong identity for government applications and associated with the user who then manages as he wishes his other identities derived from the first. The French industrial sector has all the players and skills required for this alternative (secure elements, Identity & Access Management (IAM), integration of solutions, cryptography, biometrics, PVID, etc.). The project has been taking shape since 2022 at the French level around the deployment of the National Electronic Identity Card (CNIe) and FranceConnect, and at the European level around the digital identity wallet project (eIDAS2).

One possibility for the future would be the synergy between the digital identity theme and that of data sovereignty, with the deployment in Europe of a strong digital identity, certified by a trusted public organisation and associated with derived identities centred on the user as well as with connection data - which are themselves stored in Europe and the use of which would be conditionally reserved for European players only.

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.

6.2 Specific Digital Trust innovations 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 groups together all the processes aimed, for example, at encrypting information to ensure confidentiality between the sender and the recipient. There are many technological developments in cryptography and French industry and its training and research ecosystem are at the top of the world in this field. In addition to the technological fields that are already fairly mature (public key cryptography, etc.), the main fields of innovation are as follows :

■ **Lightweight cryptography.** The rapid development of the IoT has a huge impact on all aspects of cyber security. Recent massive attacks on IoT configurations have shown that strong cryptographic techniques must be used to ensure overall system security. Unfortunately, regarding the IoT, where cost is an important parameter, the use of cryptography can be limited by the size, power and local computing performance of the objects. This has given rise to a very active research field around so-called lightweight cryptography. In short, lightweight cryptography seeks new cryptographic algorithms or protocols suitable for implementation in restricted environments, including RFID tags, sensors, health and care devices. Lightweight cryptography will progressively be used in all IoT domains where the SWAP (size, weight and power) concept tends to become critical. The first industrial applications are being developed and implemented.

■ **Post-quantum cryptography.** Communications, whether terrestrial or satellite, are central to our society and effective tools have been developed over the last few decades to secure the data exchanged and to protect against attacks. However, the quantum computer and its potential computing power represents a threat to data encrypted with these methods, which it could decrypt in record time. In response to this threat, post-quantum cryptography is based on new mathematical concepts to encrypt messages and thus secure the transport of information. In this context, The RESQUE consortium, which includes six French entities (Thales, TheGreenBow, CryptoExperts, CryptoNext Security, ANSSI and Inria with six affiliated academic institutions), has embarked on a three-year project to develop a post-quantum cryptography solution. The project aims to secure communications and infrastructures 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 post-quantum hybrid VPN and high-performance HSM. These projects extend beyond France's borders, as demonstrated by the partnership between Thales and leading Korean mobile operator SK Telecom to develop post-quantum cryptography for 5G networks.

In 2021 the ACN published a report on advanced cryptographic processes, in which the state of the art for each of these technologies is described.

ACN Report
«Advanced cryptor graphic processes»
Available on :
www.confiance-numerique.fr

■ **Homomorphic encryption.** The significant development of cloud computing has generated a very active research field around so-called functional encryption and homomorphic encryption: functional encryption is a new paradigm for public key encryption that allows both fine-grained access control and selective computation on encrypted data. In its most complete version, fully homomorphic encryption (FHE) allows computation on encrypted data without disclosing any information about the underlying data. In short, one party can encrypt some input data, while another party, who does not have access to the decryption key, can blindly perform computations on that encrypted input. The final result is also encrypted, and can only be recovered by the party that has the secret key. This field is very promising and the first industrial applications are emerging.

■ **DNA based Cryptography.** This is a new branch of cryptography. It uses DNA as a carrier of information and computation using molecular techniques. It is a relatively new field that has emerged following discoveries about the great storage capacity of DNA - which is the basic computational tool in this field. One gram of DNA stores about 108 TB of data, which exceeds the storage capacity of any electrical, optical or magnetic storage medium. The first industrial applications should emerge in the next few years.

■ **Cryptography using generative adversarial neural networks (GAN cryptography).** Generative adversarial neural networks are a recent innovation in artificial intelligence. The use of these algorithms in cryptography makes it possible to improve the quality of certain systems. This field is still at the development stage and the first industrial applications should emerge in the next few years.

2. Secure elements. This innovative field is particularly important for France because all the underlying technologies are born there, allowing the development of three world leaders from France: Thales, Idemia and ST Microelectronics. Secure elements are micro or nanoelectronic components comprising a combination of secure embedded software (SW) and hardware (HW) and designed to be integrated into communicating devices in order to securely manage all interactions between the latter and the outside world by storing dedicated applications and confidential data in an encrypted manner (SIM cards, bank card chips, etc.).
In the context of the development of IoT, the secure elements segment is marked by the replacement of SIM cards (Universal integrated circuit card) by miniaturized secure elements directly embedded or integrated in the systems to which they are attached, or even without any hardware component (soft secure elements, Trusted Execution Environment). The deployment of embedded secure elements (e-UICC) and Soft secure elements has begun and the massive deployment of integrated secure elements (i-UICC) is not expected to take place before 2024, i.e. once the problems of assurance and standardisation have been resolved. France currently leads the world in this sector with Germany and ahead of China, the United States and South Korea. The main competitors of the French players at world level are the Dutch NXP, the Germans Infineon and Gieseke & Devrient, the South Korean Samsung and the Chinese Shanghai Huahong and Shanghai Fudan Microelectronics. There is a potential medium-term threat to French players due to the lack of skills in Europe and France in More Moore technologies which is likely to lead to American and Asian manufacturers acquiring dominant positions in the i-UICC segment. Soft secure elements also represent a strong threat to French players, mainly through the American GAFAMs and the Chinese BATXs which can take advantage of their dominant position to impose their solutions.

3. Artificial Intelligence (AI). Artificial intelligence covers the development of machine learning algorithms (artificial neural networks, multi-layer or not, supervised or not, generative adversarial networks, etc.) for prediction or classification purposes, generative text AI such as ChatGPT, and the issue of edge AI, i.e. the design of chips and embedded systems dedicated to the operation of machine learning algorithms (which are very greedy in terms of computing and memory capacity). Developments in the field of artificial intelligence are not specific to the security sector, but the theme does involve setting up a framework for trusted AI.

• **The need for a legal framework:** to ensure that its development and use are in line with society's fundamental values. This involves European legislative work to establish a stable legal framework that protects both the rights and freedoms of citizens while enabling technological innovation. This framework must take into account several aspects of AI, such as its technical nature and liability, and be drawn up in a concerted manner to form a coherent and solid foundation. The challenge is to regulate, 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 trusted AI:** AI systems must be designed to be transparent, explainable and secure. Trust in these systems can be enhanced by strict cybersecurity standards and rigorous development processes to anticipate potential flaws and abuse. In addition, the data used for the learning phase of these AI models must be managed ethically, with clear standards to avoid the introduction of discriminatory biases, to ensure that the decisions made by these models are fair and equitable.

• **Social acceptance of AI:** essential, it must be cultivated through an ethical approach to its deployment. Respecting ethical principles, protecting human rights and prioritizing human well-being in the development of AI are fundamental. Public education and awareness, combined with transparent demonstrations of the usefulness and safety of AI, such as at major events, can facilitate better understanding and acceptance of these technologies.

When it comes to artificial intelligence, France benefits from excellence in training and research, and French security players are taking fairly strong positions in security applications (notably Thales Digital Identity & Security and Idemia). Although lagging behind the USA and China, who are leveraging their strong digital industrial fabric, France has a competent industry in industrial AI and generative AI. Despite this, however, there is a brain drain from France to the USA in this field, which threatens French positions in the future, including in the security sector.

The ACN publish its white paper on trusted AI in march 2024

White paper
«Trusted artificial intelligence»
Available at:
www.confiance-numerique.fr

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.

5. 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 a variety 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.

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

6.3.a 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.

Focus - CNRS, INRIA, CEA

THE RESEARCH PROGRAMME (PEPR) OF THE NATIONAL STRATEGY FOR CYBERSECURITY 10 FUNDAMENTAL RESEARCH CHALLENGES FOR THE INDUSTRY

To face an ever-growing cyber threat and increasing international competition in the development of solutions to protect citizens, businesses and institutions, France has adopted a national cybersecurity strategy as part of the France 2030 investment plan. The objectives are to triple the industry's turnover by 2025, train more professionals and develop sovereign solutions at a time when cybersecurity issues are becoming ever more pressing.

Goals:

Funded to the tune of €65 million over 8 years, the Cybersecurity research programme (PEPR) supports fundamental research activities at the highest international level. The results of this program feed into the more downstream actions of this national strategy, such as the Cyber Campus Transfer Programme (PTCC), the CyberBooster incubator, the Grand Défi Automatisation de la Cybersécurité, and calls for projects for the Development of Critical Innovative Technologies, among others.

Officially launched in June 2022, this PEPR aims more specifically to:
- Launch and fund scientific challenges in fundamental research;
- Structure research communities;
- Achieve scientific breakthroughs in cybersecurity;
- Develop breakthrough technologies that will benefit all French players in the sector;

A Shared governance, a mobilised academic community

Carried out in close collaboration with the national research community, the scientific steering committee has been entrusted to the CEA, CNRS and Inria.
The framing of this PEPR has benefited from a major mobilisation of the entire scientific community, as well as the major state and socio-economic players. It now involves more than twenty universities and prestigious universities, representing a total of 300 researchers.

To favor the valorisation of knowledges, technologies and tools developed by the PEPR Cybersecurity and to create synergies with the other actions of the national cybersecurity strategy and with other acceleration strategies (Quantum, AI, Cloud, Networks of the Future, TASE, Digital Health), the PEPR Cybersecurity has set up a governance structure. Its aim is to involve socio-economic players as effectively as possible in defining its strategy and in diffusion and communication activities.

The governance bodies are as follows:

- Steering Committee (COPIL), responsible for the strategic management of the programme
- Programme Management (CODIR), responsible for programme coordination
- Programme Committee (COPROG), responsible for programme management
- Strategic Orientation Council (COS), made up of academic and socio-economic players, consulted each year to give an opinion on the programme and revisions to the roadmap.

Presentation of the ten research projects launched since 2022:

- Protection of personal data (IPoP)
- Secure data processing in the cloud (SecureCompute)
- Security of protocols and electronic voting (SVP)
- Multimedia data security (COMPROMIS)
- Malware defence (DefMal)
- Security supervision and orchestration (SuperviZ)
- Hardware and software security for embedded systems (ARSENE)
- Software security evaluation (SecurEval)
- Resistance of cryptographic systems (Cryptanalyse)
- Exploitation of vulnerabilities in digital forensics (REV)

Production, main spin-offs, and influence of the PEPR Cybersecurity programme

The «PEPR Cyber Day» is a scientific seminar organised each year to present the latest results from the programme's projects to industry and the State, and to discuss their use and transfer. Since its launch in 2022, PEPR has already produced:
- 120 world-class scientific publications
- 40 PhD students recruited
- 31 post-docs and engineers recruited
- 37 scientific seminars
- 45 events for the public
- 2 start-ups in the process of being created
- 1 grant from the European Research Council accepted and several Horizon Europe projects in the pipeline
- Software and platforms developed,
- 2 researchers awarded scientific prizes: Véronique Cortier (CNRS Silver Medal 2022), Anne Canteaut (Irène Joliot-Curie Prize 2023).

To contact PEPR Cybersecurity: contact@pepr-cybersecurite.fr

To follow PEPR Cybersecurity: www.pepr-cybersecurite.fr

To subscribe to PEPR Cybersecurity's quarterly newsletter: https://evento.renater.fr/survey/newsletter-programme...-b1ixhs1z

6.3.b 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

6.3.c ...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 Etudes & 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).

6.3.d ... 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 Etudes & 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.

ABOUT ACN

The Digital Trust Alliance (Alliance pour la Confiance Numérique - ACN) represents companies (world leaders, micro-entreprises, SMEs and ISEs) in the digital trust industry and in particular those in digital identity, cybersecurity and trusted AI. France has a highly efficient industrial fabric in this field and an internationally recognized excellence thanks to world leaders, SMEs, ISEs and the various dynamic players in the sector.

There are 2,178 companies with a revenue of €19 billion in France in this fast-growing sector (8% average annual growth since 2016).

The 120 members of the Alliance pour la Confiance Numérique (ACN), 87% of which are Micro-entreprises/SME-ISEs, account for 2/3 of the revenue of French digital trust companies worldwide (hardware manufacturers, software publishers, integrators, services, security assessment laboratories, research, etc.).

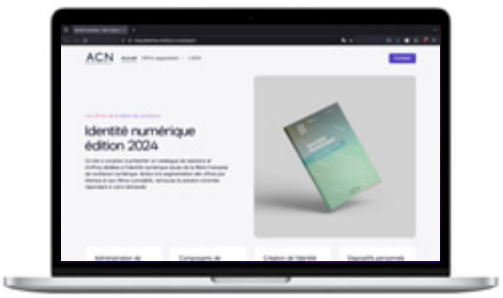
ACN is a member of the FIEEC (Fédération des Industries Electriques, Electroniques et de Communication), is an associate member of the Cyber Campus and actively participates in the work of the CSF (Comité Stratégique de Filière) of the Security Industries.

ACN is also a founding member of the association representing the European cybersecurity ecosystem: ECSO (European CyberSecurity Organisation).

Last Publications :

New: ACN has launched a website to list French digital identity digital identity services:

https://identite.confiance-numerique.fr/



ACN
Alliance pour la confiance numérique

@ACN_SecNum ACN - Alliance pour la Confiance Numérique ykassianides@confiance-numerique.fr

ACN Members :

ACN Partners :

ABOUT DECISION

Since 2017, DECISION has conducted the Observatory of Digital Trust for the ACN.

DECISION is an independant strategy consulting firm specialised in economic studies (market analysis, forecats, value chain, etc.) in specific areas:

• Electronic (components, equipment, systems) ;
• Aeronautics, Defence, Security ;
• Electric, Renewable energies and the Industry of the future.

Our clients include private companies, whether start-ups/SMEs/ISEs, large industrial groups, professional organisations or financial institutions and investment funds, but also 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 of the executive contract (2010-2015) on the security industry (including cyber security) for the DG ENTR of the European Commission.

Since then, DECISION has also carried out studies to evaluate the economic weight of the security sector 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 the CoFIS (Comité de la Filière Industrielle de sécurité), bringing together the Ministry of the Economy (DGE), the Ministry of the Interior (DMISC), the SGDSN, the CICS (Conseil des Industries de la Confiance et de la Sécurité), the GICAT and Milipol.

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

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

DECISION
ETUDES & CONSEIL

Graphic Design / Theo Broyer Alran & Arthur Pajaud.

French version available on :
www.confiance-numerique.fr

Press Partner