2023

Alliance pour
la confiance numérique

confiance-numerique.fr

Observatory of Digital Trust Sector

ACN
Alliance pour la confiance numérique

CONTENT PAGE

A WORD FROM ACN - ALLIANCE FOR DIGITAL TRUST

Daniel Le Coguic
ACN Chairman

More than ever, Digital Trust is at the heart of the challenges facing our societies. Digital technology is tending to become the preferred mode for all our exchanges, in our daily lives, in our economic activities, in our relations with the State, but also in the geopolitical sphere. In this respect, the digital space is becoming more and more the expression ground for all the behaviors and needs that are usually the prerogative of the physical world, the latter being accelerated, multiplied and dematerialized. Trust has been the cornerstone of human relations since man first organized himself into communities. It is the basis of all communal life, and it structures the legal edifices of every society, whether to govern interactions between individuals, or to ensure public or international order. Since its creation, the digital age has been built essentially on an utilitarian vision: its power and massive broadcast are now calling into question our societies and our operating rules, which were designed to regulate physical interactions. However, to regulate digital technology by only tackling its dystopian effects once they have been observed is to treat the symptoms rather than the causes, and thus condemns us to a perpetual backwardness and maladjustment of the responses we provide. It's urgent to get back to the fundamentals and establish as an intangible principle that trust in digital technology is the basis for its deployment. The tools that contribute to Digital Trust are numerous. Digital identity is a key: in the physical world, as in the digital world, there can be no trust if you can't be sure that you're dealing with the right person. Cybersecurity is also a major focus: we need to be sure that digital interactions take place as intended, without intrusions or distortions, and without the possibility of interrupting them.

Finally, the power of artificial intelligence must imperatively be controlled and regulated by this Digital Trust. It is the primary ambition of the «Securing and Regulating the Digital Space» bill, with measures to protect our fellow citizens, especially children, our businesses and communities, and our democracy. These measures, presented by Minister Jean-Noël Barrot, call for many others. ACN supports the holistic vision that has been adopted. This vision has societal, economic, democratic, and geopolitical implications. As at the European level, the time has come to develop rules designed to achieve the same objectives of regulating and

securing the digital space. Under the aegis of Commissioner Thierry Breton, numerous initiatives are underway (NIS2 directive, Cyber Resilience Act, draft regulations on a European portfolio of digital identities, AI Act project, etc.). France is fortunate to have all the tools at its disposal to strengthen its digital sovereignty, control its digital future and decisively contribute to the French and European strategic autonomy. The Digital Trust industry is made up of a solid, dynamic and agile ecosystem of companies, from world leaders as well as start- ups and SMEs of excellence.

Every year for over 10 years, ACN has used its Observatory to track developments in the industry and decipher its main trends. In 2022, the Digital Trust industry experienced its strongest growth since 2015 (+10.1% in sales). This growth, 3 points higher than the average rate of increase over the last 5 years, confirms the analysis of a sector driven by very solid underlying trends such as digital transformation, the development of telecommuting, the maintenance of threat levels at a high level, the regulatory context and the growing awareness of companies and institutions... This momentum must not, however, mask the scale of the challenges facing us: in order to meet the numerous needs, identified and to come, to protect our country, improve the security of all, and preserve our digital sovereignty, the French Digital Trust industry must succeed in attracting and training talents, but must also structure itself efficiently. The stakes are both national and European, and the influence we can exert on this scale depends on our ability to concentrate our efforts and take collective, coordinated action. It is precisely the role of a professional organization such as ACN to ensure the synergy and institutional representation.

In the digital world, much remains to be written, and our sector is convinced that it can show an original way forward in an increasingly conflictual, multipolar world. This path consists in bringing together fundamental French and European values and the Digital Trust tools that ensure their continuity and promotion. A watchword for the industry: to develop and to make to provide tools that are compatible with public freedoms and acceptable to our fellow citizens. Capitalizing on our strengths and on the excellence of the French Digital Trust industry will not only protect us and make us more resilient, but also strengthen our social model. The French government must continue and expand its efforts to support our young, dynamic industry, so that it can become the pillar of our digital sovereignty. In an increasingly conflictive geopolitical context, where the various blocs do not share the same values, it is time to work collectively to strengthen France’s voice for a more peaceful, freer, more innovative and more protected digital Europe, for the benefit of the greatest number. Let’s work together to build this new France, which will become the spearhead of the European project.

A WORD FROM THE MINISTER

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

Jean-Noël Barrot
Minister Delegate for Digital Transition and Telecommunications

The digital transformation of the French economy and flourishing availability of connected objects combine to multiply cybersecurity risks at a time when the geopolitical context is particularly conducive to cyberattacks capable of destabilizing the economy and society. Protecting companies from cyber risks, including those outside vital sectors, has become more than ever a vital economic and national security imperative.

In this respect, the digital trust sector plays a valuable role in accommodating and supporting the digital transformations of our economy and society, while enabling our fellow citizens to benefit from a safer and more secure digital environment. The sector naturally enjoys the support of the French government, which has made it a top priority to protect the information systems of companies and public bodies, and intends to rely on a robust, sovereign and innovative private ecosystem to achieve its goal.

Aware of the stakes involved in ensuring our country's resilience in the face of the threat, the President of the Republic unveiled in January 2021 a cybersecurity acceleration strategy, backed by €1 billion in funding from the France 2030 plan. As part of this strategy, we aim to support the growth of our French and European cybersecurity industry, and to create leaders capable of reinforcing our sovereignty over these strategic technologies.

In addition to a strong focus on R&D and talent training, this strategy, for which close to €400 million in public funding has already been committed, also aims to develop innovative solutions through a specific series of calls for projects.

Among the topics covered are the development of components that secure communication tools and collaborative suites, and cybersecurity solutions for major events. In total, the strategy has supported 30 projects for approximately €85 million, with the next call for projects set to be published in June 2023.

But there are myriad ways to address the threat, and technological innovation alone is not enough. Knowledge and awareness are also key. This is why the government is particularly committed to coordinating and decentralizing its efforts, to be

more efficient in addressing needs at a regional level.

This is the entire purpose of the Cyber Campus in 2021, the flagship of our ecosystem that will strengthen the synergy between public and private stakeholders. This is also the case for the cybersecurity courses that the ANSSI has piloted for the benefit of close to 1,000 public organizations, and which directly contribute to making our public services more cyber-resilient.

As part of my efforts to raise awareness among economic players, I also announced last October a grant to fund 750 sensitive SMEs and SMBs in their cybersecurity efforts, on the basis of three main principles: an end-to-end approach that takes into account the cyber maturity of organizations, targeted recruitment by sector, and a strong link with the regions. The construction work for this program is nearing completion and we will be able to welcome the first applications from eligible organizations over the summer of 2023.

The socio-economic and sovereignty issues relating to artificial intelligence have recently been in the spotlight.
For AI to be «trusted», it must guarantee the absence of failures, the safety of users and the reliability of systems. In order for this to occur, the way algorithms operate must be safe, explainable and responsible, especially for systems that may involve human lives or infringe on the rights of individuals. This is an essential prerequisite for any technology to be adopted by citizens.

It is essential to equip ourselves with technological solutions that will enable the French ecosystem to develop products and services compliant with the requirements of the future European regulation (AI Act). Indeed, beyond investment, the development of trusted AI will also require the implementation of a clear and appropriate regulatory framework. France, which actively participated in negotiations on the AI regulation during its presidency of the Council in the first half of 2022, was able to ensure that a balance was struck between innovation and protection.

Ethically speaking, the review process should also be formalized. This is why I recently referred the matter to the national digital ethics committee, which the President of the Republic rendered permanent on March 9th to mark the 40th anniversary of the national ethics advisory committee. The conclusions of the referral will be submitted to the Government before summer.

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 Confiance Numérique (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 2023, covering the field of cybersecurity and digital security.

Digital Trust in France in 2022 corresponds to :

€17.7 billion in revenue in France

- **€17.7 billion in revenue**, i.e. 10.0% growth between 2022 and 2021
- **€8.4 billion of added value**
- **86,700 people employed** in the sector
- **56% of revenue** from **cybersecurity** and **44% from digital security**

French Digital Trust companies in the world in 2022 represent :

€16.4 billion in international revenue

- **€28.7 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 capital)
- **World leaders** in digital security (Thales, Airbus D&S, Atos, ST Microelectronics), identity and access management (Thales, Idemia, IN Groupe, Docaposte), cybersecurity services (Thales, Atos, Orange Cyberdefense, Sopra Steria, Capgemini), and secure payments (Worldline)
- **€16.4 billion in international revenue**, i.e. 57% of total revenue (revenue exported from France and revenue generated abroad by companies owned by French capital)
- **€5.4 billion of revenue exported from France**, an average export rate of 31%.

Digital Trust is a thriving industry :

10.1% growth in France in 2022

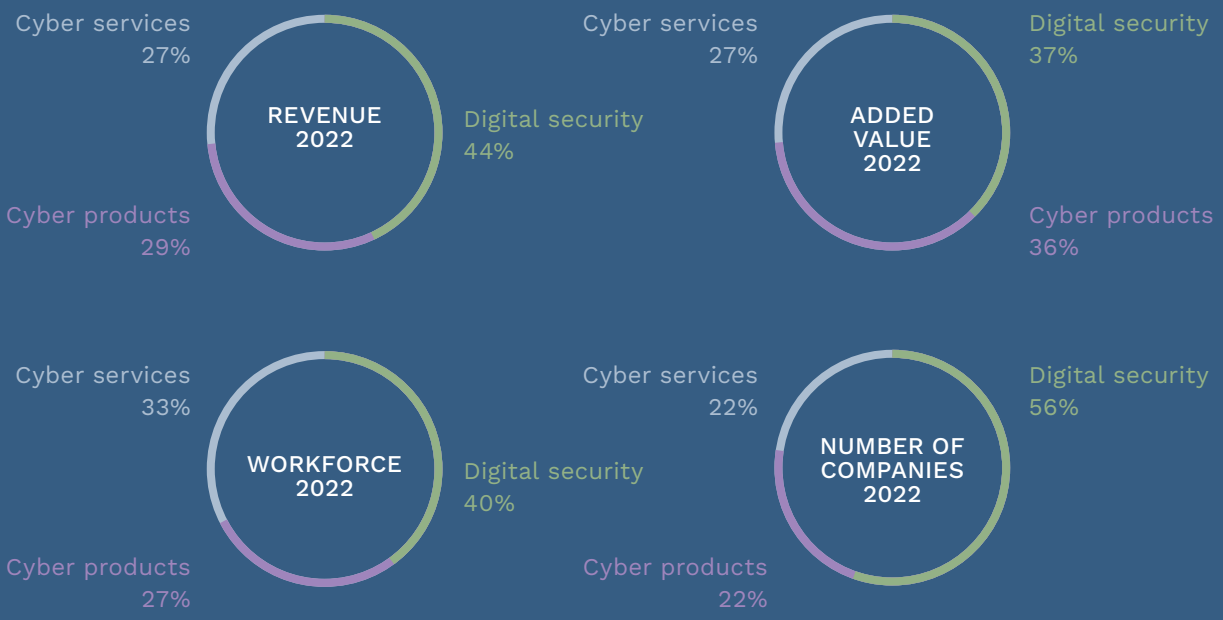
- **7.5%** average annual growth in France over the 2017-2022 period, compared to 1.0% for the French GDP (GDP growth measured by INSEE in chained volume, IMF for the year 2022);
- Digital Trust is the **French industrial sector that has experienced the strongest growth over the past 10 years;**
- **Digital 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 :

2,129 companies in the sector in France

- **2,129 companies** in the sector in France;
- Of which **75 are large entreprises;**
- Of which **67 ISEs** (Intermediate-sized enterprises);
- Of which **644 SMEs** (Small and Medium-sized Enterprises);
- Of which **1,343 Micro-entreprises,** generating less than 2 million in revenue in 2022.

Main sectors in Digital Trust



Sources : DECISION études et conseils

KEY FIGURES 2022

Revenue

€28,7 B of global revenue

- €11 B of revenue abroad
- €17,7 B of revenue France
  - Included €5,4 B of exported revenue

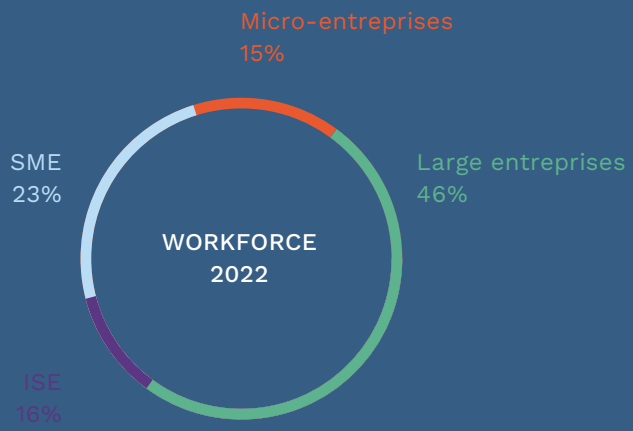
€8,4 B AV* France

*(added value)

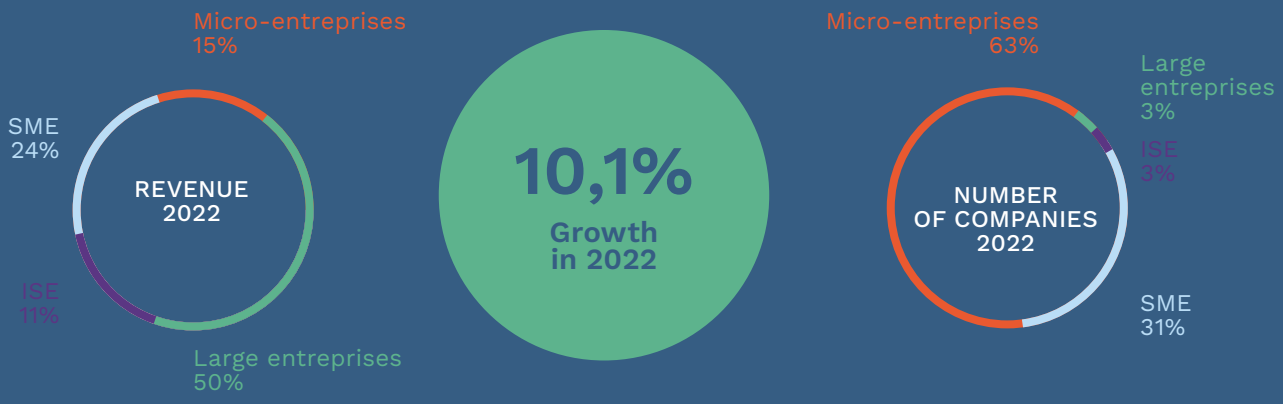
Workforce

86 700
Workforce in France in 2022

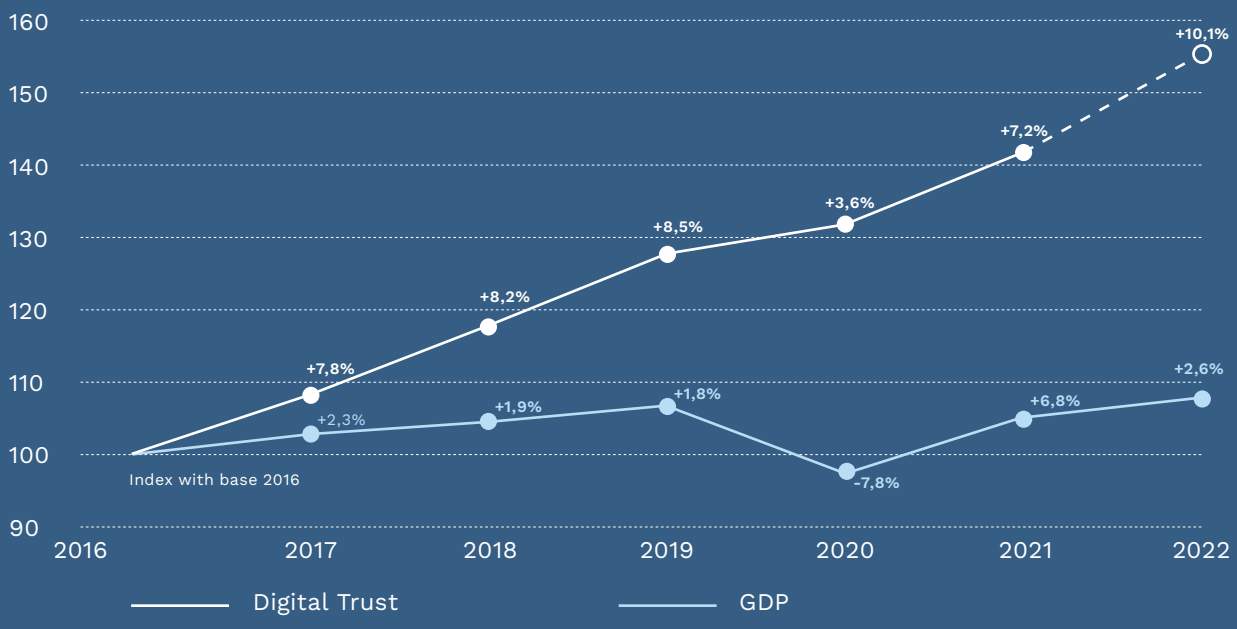
138 100
Workforce abroad in 2022



Growth



France growth comparison 2017-2022

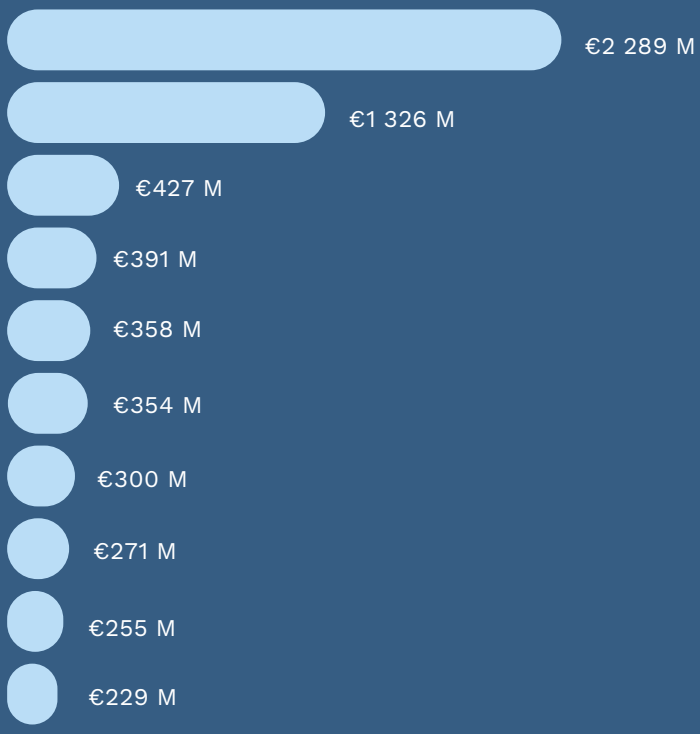


GDP growth measured by the INSEE and IMF for 2022.

Source : DECISION Etudes & Conseils

Top 10 players France 2022

N°	Company	Digital Trust revenue France
1	**THALÈS**	€2 289 M
2	**AIRBUS**	€1 326 M
3	**ATOS**	€427 M
4	**ORANGE CYBERDEFENSE**	€391 M
5	**IDEMIA**	€358 M
6	**DOCAPOSTE**	€354 M
7	**IBM**	€300 M
8	**IN GROUPE**	€271 M
9	**ACCENTURE**	€255 M
10	**SOPRA STERIA**	€229 M



- 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 and Leidos Cyber.
- Docaposte includes AR24, CDC Arkhineo, Open Value...
- Accenture includes Arismore, Link by net, Openminded...
- Chapvision / Flandrin technologies includes Deveryware, Bertin IT, Vecsys and Elektron.
- Idemia includes Otono Networks.
- IN Groupe includes Surys and Nexus.
- Econocom includes Exaprobe.
- Wordline includes Ingenico.
- GFI Informatique includes SIS.
- Cisco includes Sentryo.
- Securitas includes Stanley Security.
- Sogetel includes Eryma.

Emergence of an ecosystem of cybersecurity products and services providers

Top 1-10 players in France

Top 10-20 players in France

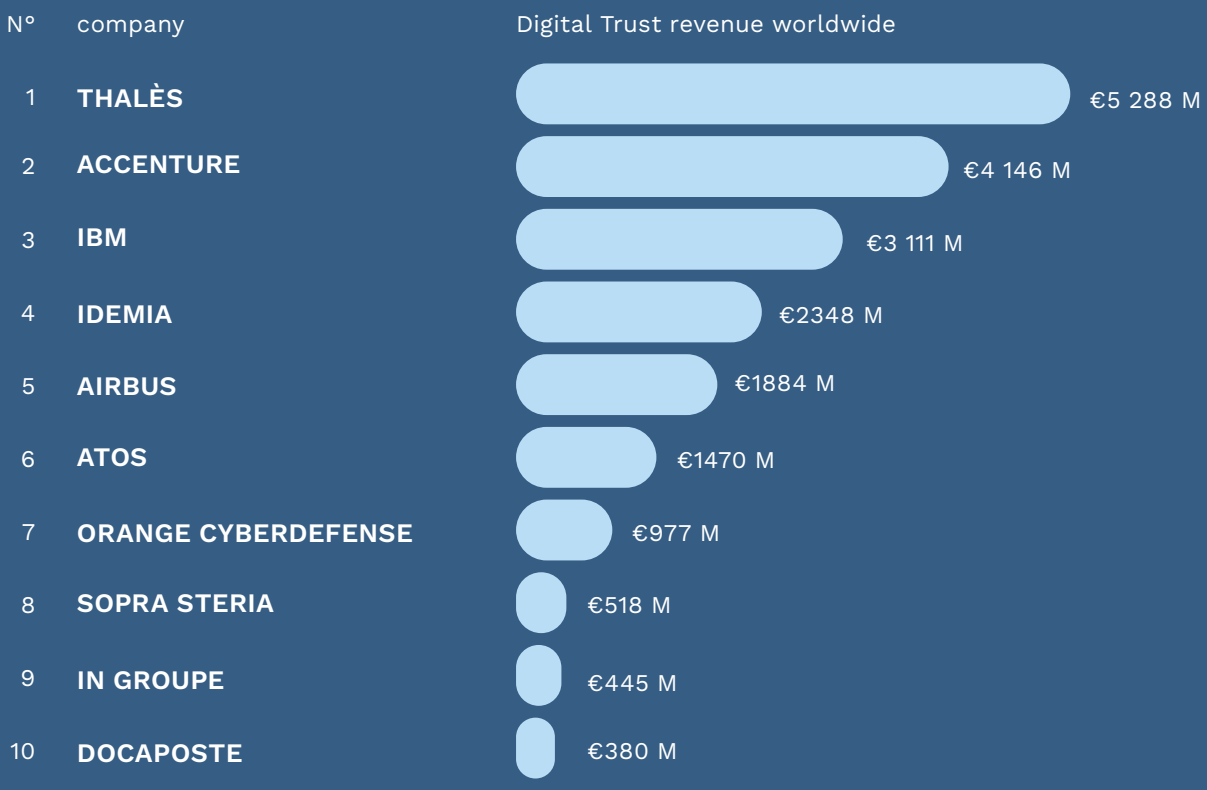
French Digital Trust revenu in between €100M & €230M

Top 20-50 players in France

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

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

Top 10 players worldwide - 2022



The Digital Trust sector in France benefits from 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** entered the TOP 10, driven by strong growth and numerous acquisitions (Arismore, etc.)

ACN IS AT THE CORE OF THE INDUSTRY

Among the ACN members there are :

■ **14 large entreprises or ISE, including the 10 French leaders in Digital Trust.**
■ But also **92 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 €100 M from France in 2022, we find -in addition to Cap Gemini- French players such as Worldline (payment security), Safran (digital security), Naval Group (cyber onboard ships), Crosscall (secure communications) and STMicroelectronics, but also foreign players: Assa Abloy (access control), Linxens (smart cards), Fortinet (cyber products), and Econocom (cyber services).

The companies between 10th and 50th position have French digital trust sales that are all around €40 M: Somfy, Securitas (Stanley Security), Serma Safety & security, Schneider, Honeywell, Palantir, Devoteam, SAP, Oracle, Apixit, Inetum, DXC, Claranet, Neurones, 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 development 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 secured 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).

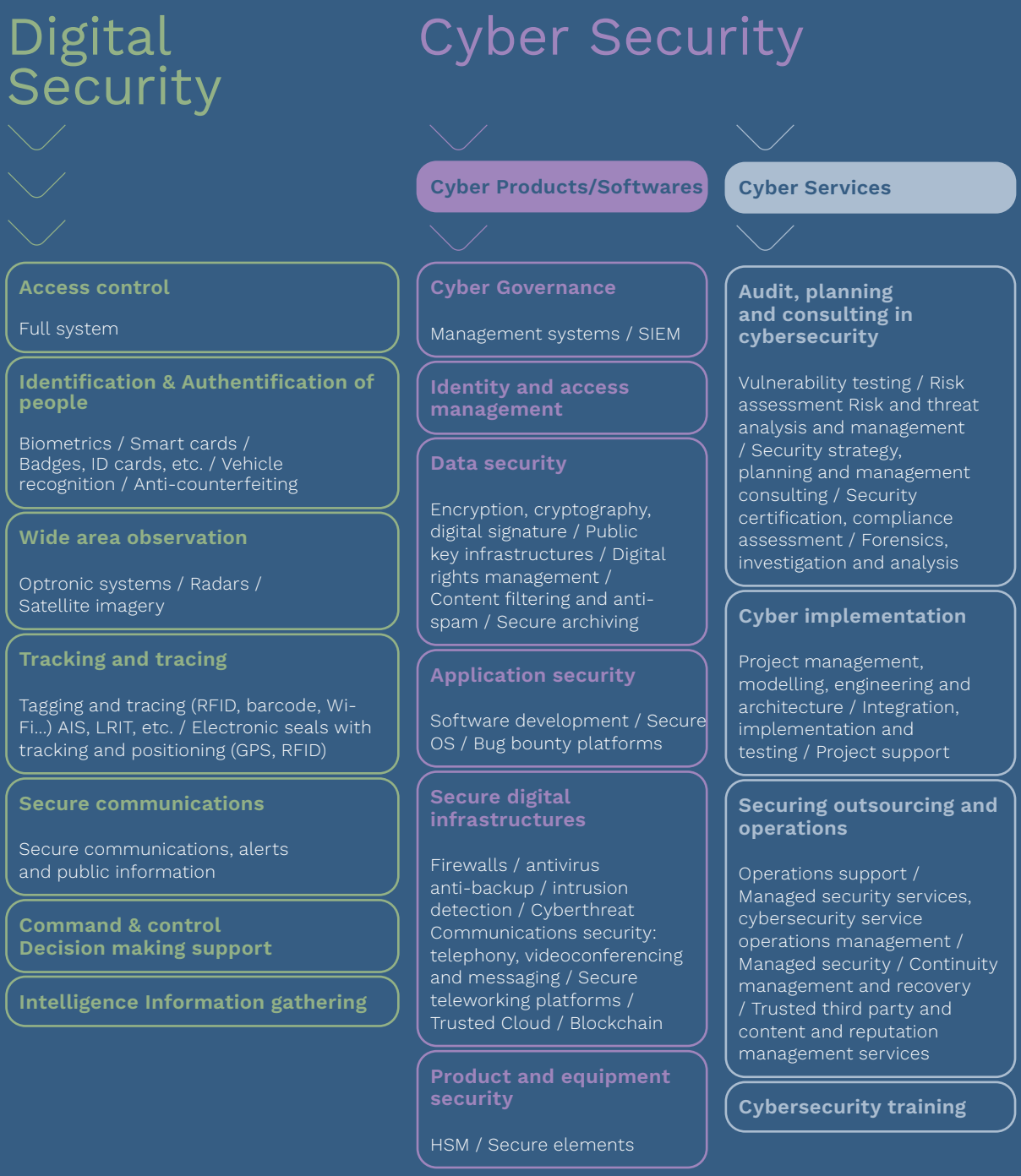
The **Observatory of Digital Trust** covers two industries:

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 equipment (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:



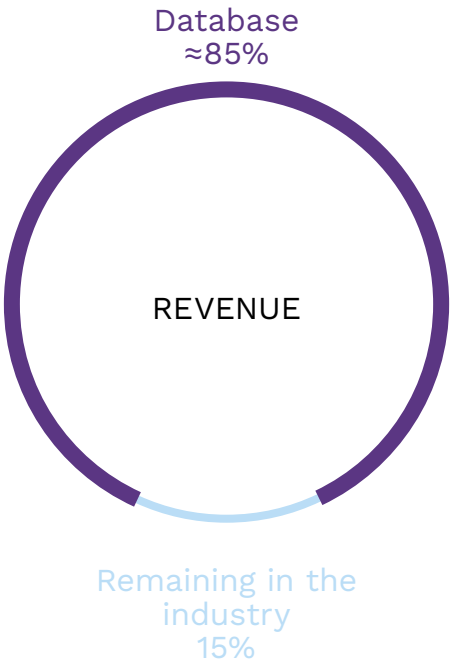
1.3 Methodology

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

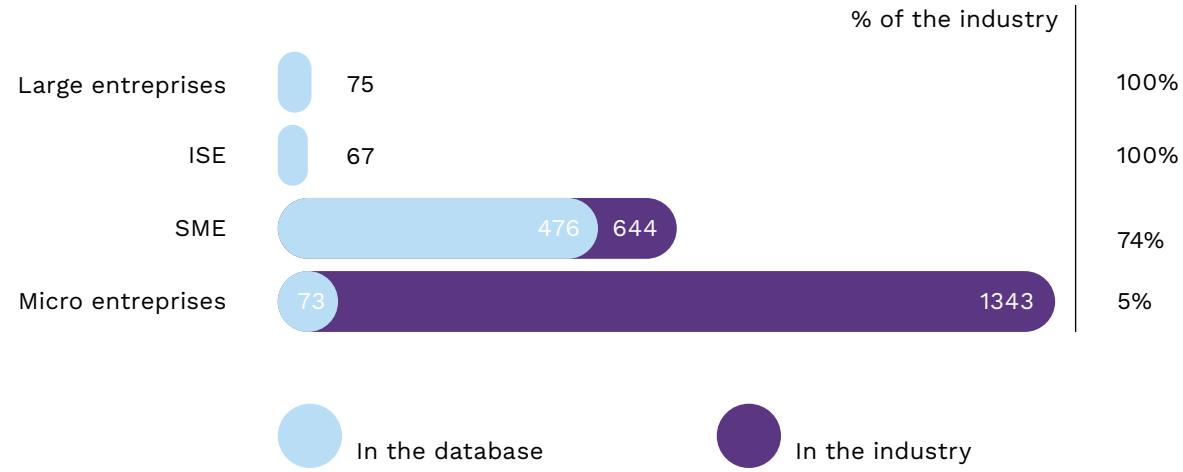
DECISION Etudes & Conseil has been conducting this Observatory since 2017. The data presented in this report are taken from a DECISION's database listing 691 companies out of the 2,129 that make up the Digital Trust sector. This database takes into account:

- All large entreprises in the sector (75/75);
- All the intermediate-sized entreprises (ISEs) in the sector (67/67);
- The majority of small and medium-sized enterprises (SMEs) in the sector (476/644);
- The most remarkable and innovative micro-enterprises and startups (73/1343).

Thus, although only 32% 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 2015-2022: 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 survey filled in each year by the industry members provides data on the growth of the past year. For the 2023 edition, the members who answered the survey represent 5% 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 survey.

Consequently, **the figures in absolute value of each edition of the Observatory are not directly comparable**. The figures of this Observatory are presented for the year 2022 and according to the new segmentation of the actors. The updated 2021 figures are presented on chapter 3.5 of this report.

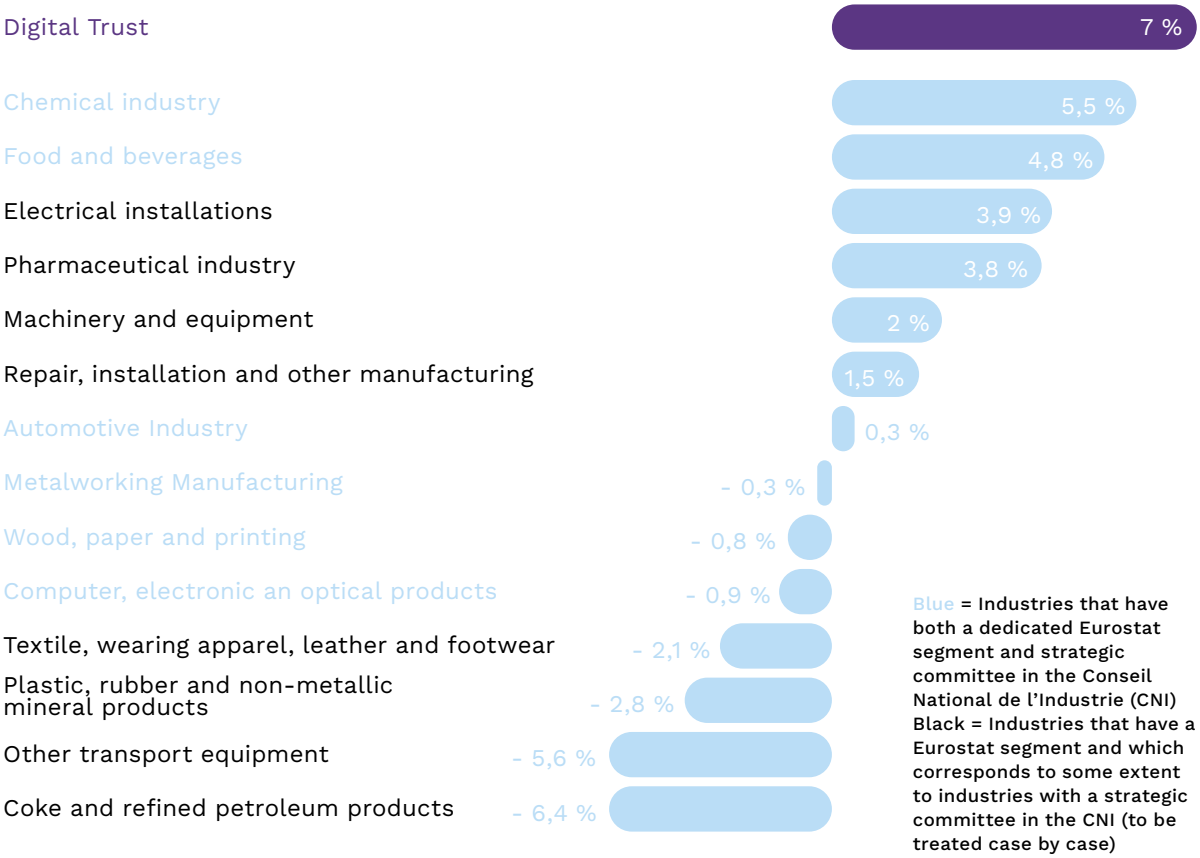
II. DIGITAL TRUST: AN IMPORTANT AND DYNAMIC INDUSTRY

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

Over the 2016-2020 period, Digital Trust is the French industrial sectors with the highest growth rate, with an average of 7%/year. Although measured using a method that is not directly comparable, the only other French industrial sectors that experience similar growth are the chemical industry and the electrical equipment industry. The other sectors are far behind, notably the automotive industry, which has suffered particularly since the COVID crisis in 2020, and the metallurgy industry.

Digital Trust is one of the four sectors (out of a total of fifteen) not to have suffered from a recession in 2020. With a growth of 4.5% that year, it is the sector that best resisted the COVID crisis and its consequences. This resilience reflects the continuing need for Digital Trust goods and services. To the extent that by 2030, Digital Trust could become the 11th out of 15 French industrial sectors in terms of added value, overtaking both the electrical equipment sector and the wood, paper and printing sector

Average annual growth of french industries over the 2016-2020 period



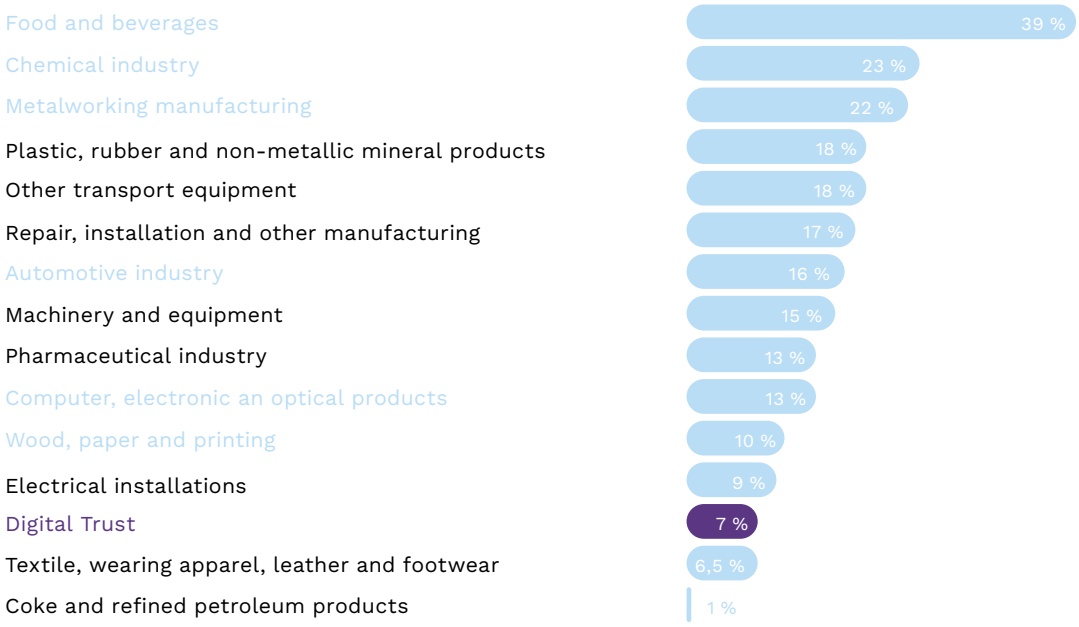
Blue = Industries that have both a dedicated Eurostat segment and strategic committee in the Conseil National de l'Industrie (CNI)
Black = Industries that have a Eurostat segment and which corresponds to some extent to industries with a strategic committee in the CNI (to be treated case by case)

Source : DECISION, based on Eurostat data until 2020 and INSEE figures on the evolution of the Industrial Production Index (IPI) over the 2019-2021 period.

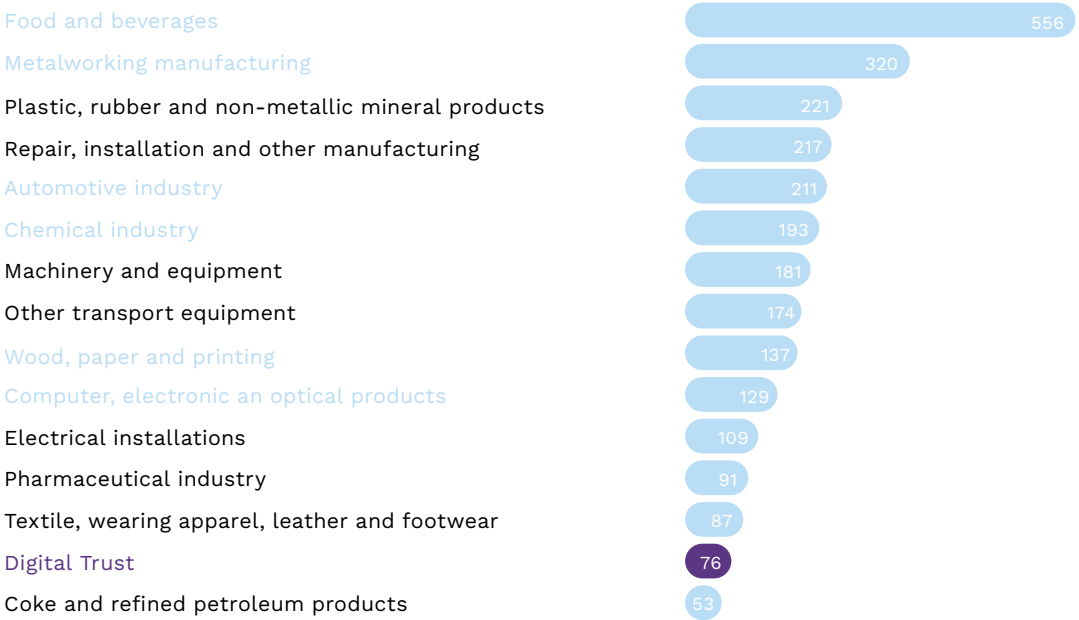
2.2 Digital Trust is a fully-fledged French industrial sector

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 equipment 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 2020 (€ Billion)



Workforce in french industries in 2020 (in thousands)



Blue = Industries that have both a dedicated Eurostat segment and strategic committee in the Conseil National de l'Industrie (CNI)
Black = Industries that have a Eurostat segment and which corresponds to some extent to industries with a strategic committee in the CNI (to be treated case by case)

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.

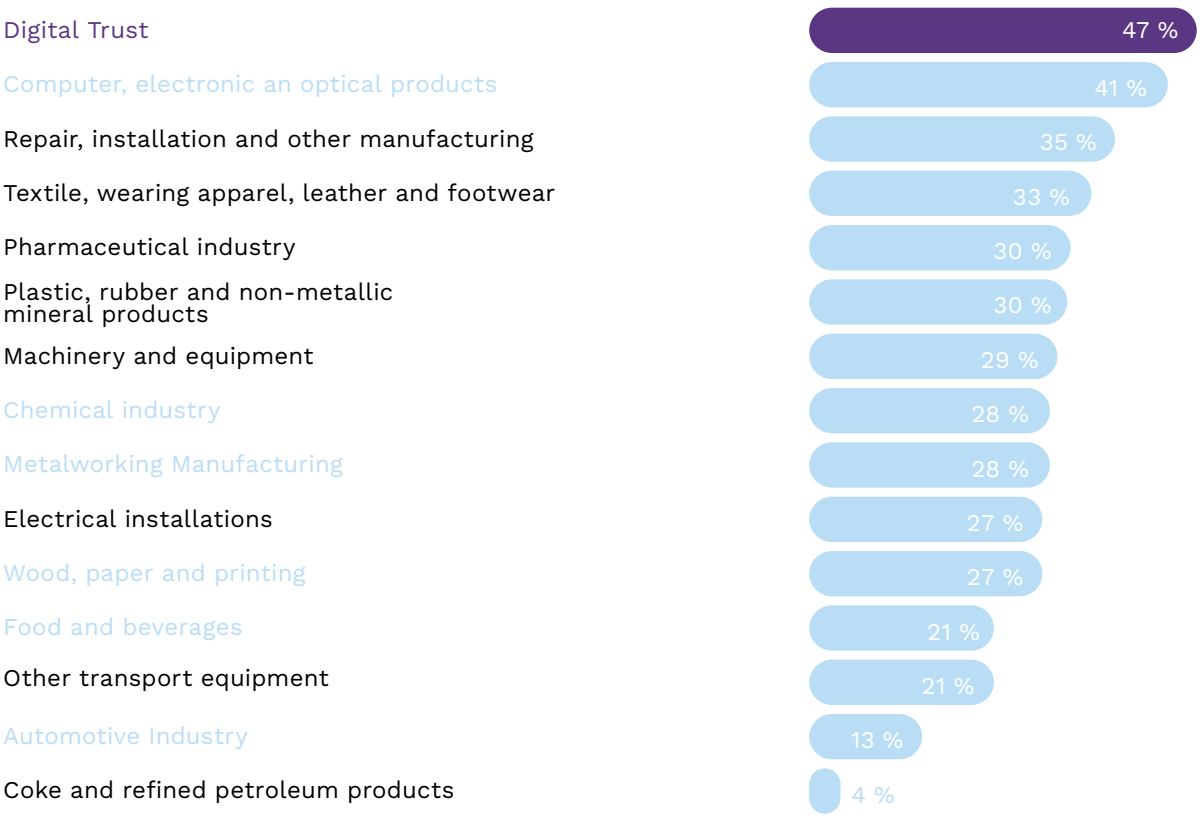
This phenomenon is mainly explained by three factors:

1. **The percentage of activity dedicated to services is relatively high in the French Digital Trust sector** (27% in 2022), through cybersecurity services (consulting, auditing, training, etc.). By definition, service activities have a very high added value rate because they use very little intermediate consumption and correspond almost exclusively to the transformation of products during the activity. However, this phenomenon alone does not justify the French security industry being the leader in terms of value added rate, as most of the French industrial sectors also include a significant part of services.

2. Electronic products dedicated to Digital Trust (digital security) correspond to 44% of the total revenue of the Digital Trust sector. However, while for the French electronics industry as a whole, a large part of the production stages upstream of the value chain is carried out in Asia, **this phenomenon hardly applies to the Digital Trust segment, which maintains all the production stages in France as much as possible because of its proximity to the sovereign sectors**. Other French sectors focus more strongly on integration activities upstream of the value chain and on pure engineering activities (design, development, etc.). As a large part of the value chain of the digital security industry is carried out from France, the rate of value added increases.

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

Added value rate (added value/revenue) of french industry 2020



Blue = Industries that have both a dedicated Eurostat segment and strategic committee in the Conseil National de l'Industrie (CNI)
Black = Industries that have a Eurostat segment and which corresponds to some extent to industries with a strategic committee in the CNI (to be treated case by case)

Source : DECISION, based on Eurostat data until 2020 and INSEE figures on the evolution of the Industrial Production Index (IPI) over the 2019-2021 period.

2.4 French players are at the top level in terms of skills and R&D

Thanks in particular to French excellence in research and development, **the vast majority of French Digital Trust companies are positioned in the high-end segments of their markets, offering solutions at the cutting edge of what technology makes possible today**. France excels particularly 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. 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 equipment on a large scale and therefore contributes to a strong growth in volume of electronic security equipment. 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**.

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 developments, 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 development 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 competition from foreign players

French players generate 75% of the Digital Trust revenue in France, i.e. €13.3 billion in 2022. In other words, **foreign players in the sector generate 25% of the sector's revenue in France**, i.e. approximately €4.4 billion in 2022. 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 development of American players in France, notably through the installation of new headquarters : Microsoft, Dell, Palantir, Docusign, AWS, Google, Splunk, Check Point Systems, Crowdstrike International, Juniper Networks, Nutanix, F5 Networks, Palo Alto Networks, Rubrik, Okta, Netskope, Forescout technologies, Aruba, Imperva, Tufin Software, Quest software, Proofpoint... Chinese players are also developing, recently with highlevel offers capable of competing 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) and 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 competitive 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 competition 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 any other French industry ;
- Digital Trust is already of a **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.

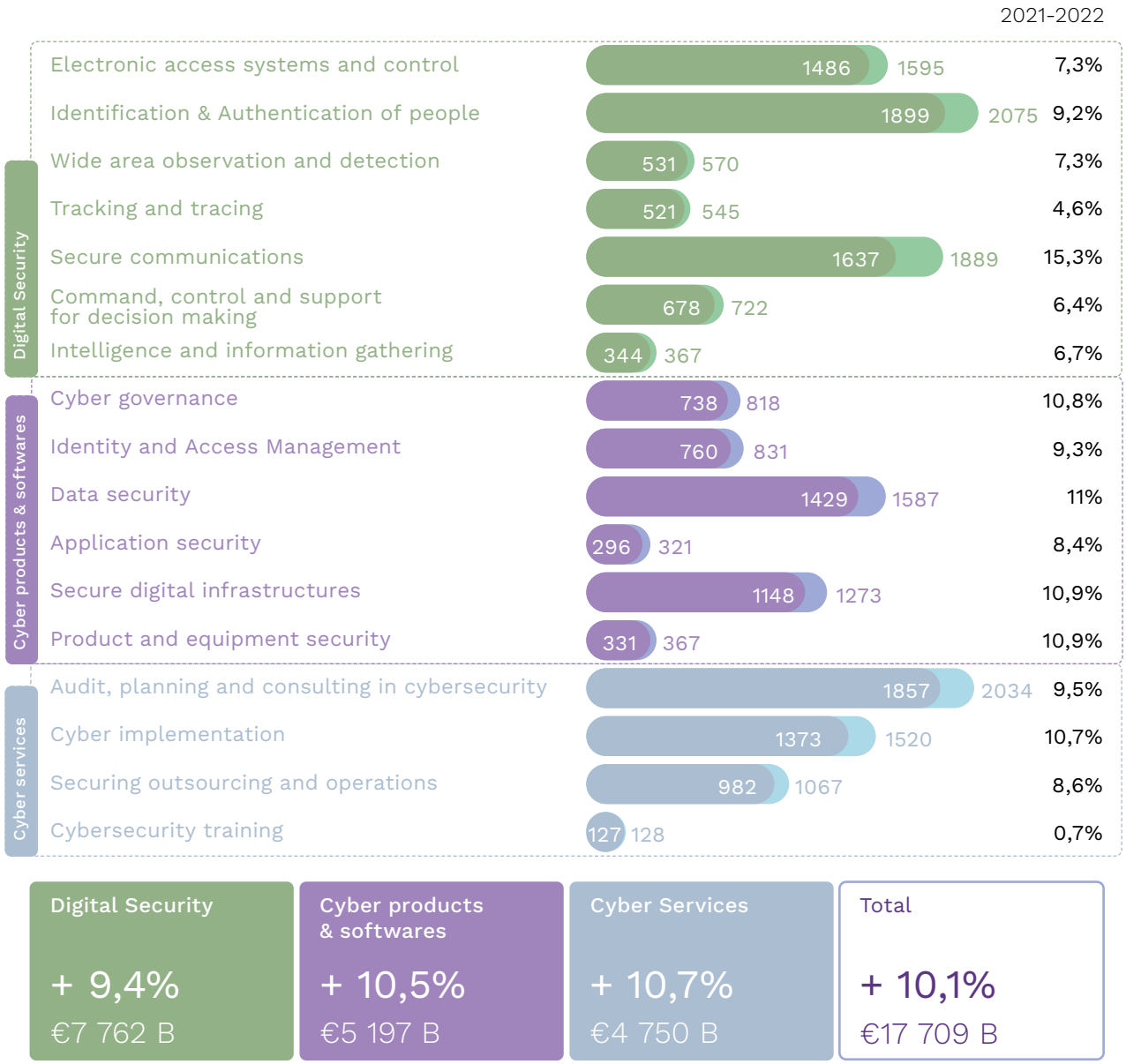
III

KEY FIGURES OF THE INDUSTRY

III. KEY FIGURES OF THE INDUSTRY

3.1 Size and growth

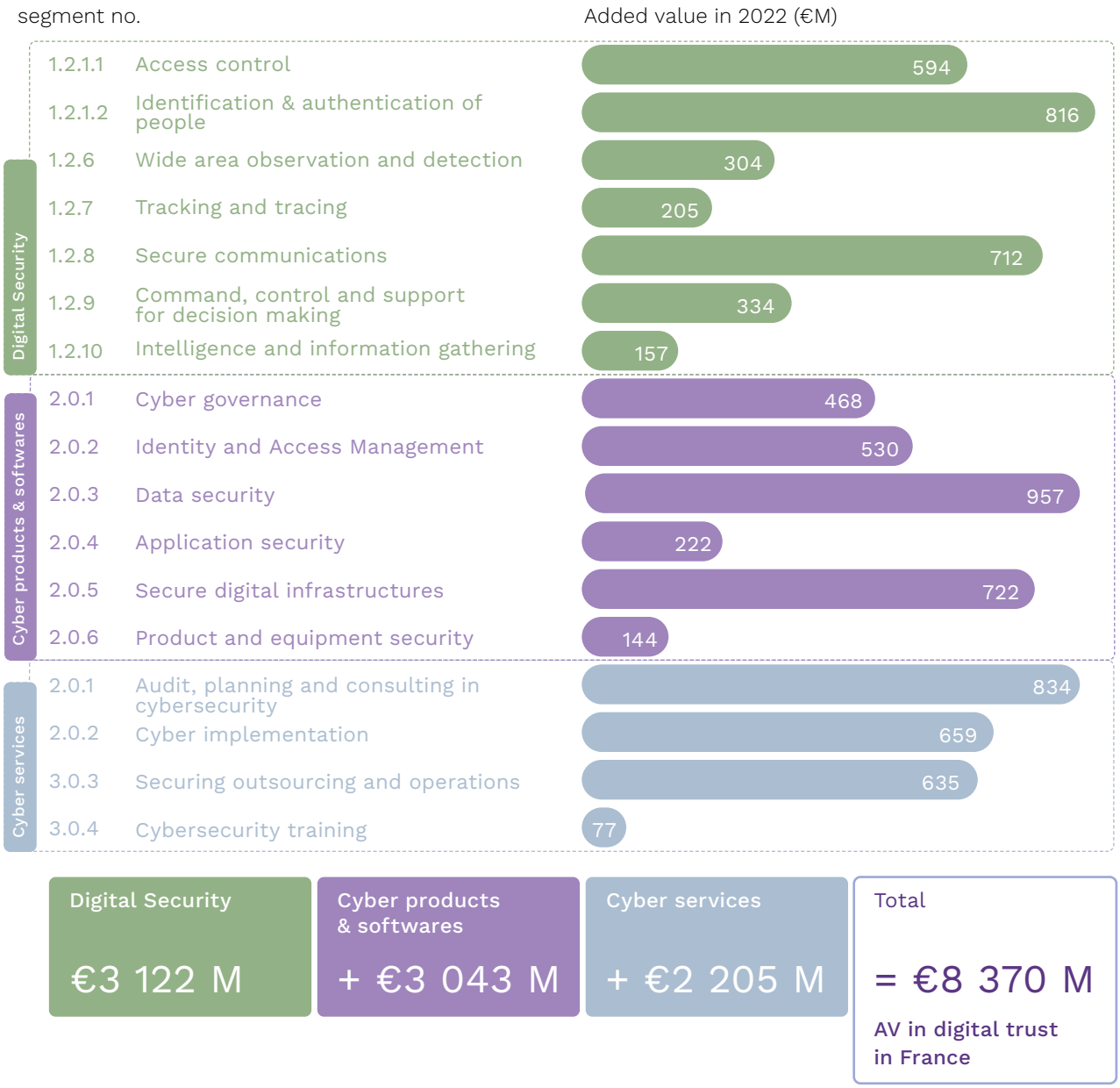
Revenue of Digital Trust in france € 17,7 B in 2022



Digital Security	Cyber products & softwares	Cyber Services	Total
+ 9,4%	+ 10,5%	+ 10,7%	+ 10,1%
€7 762 B	€5 197 B	€4 750 B	€17 709 B

3.2 Added value

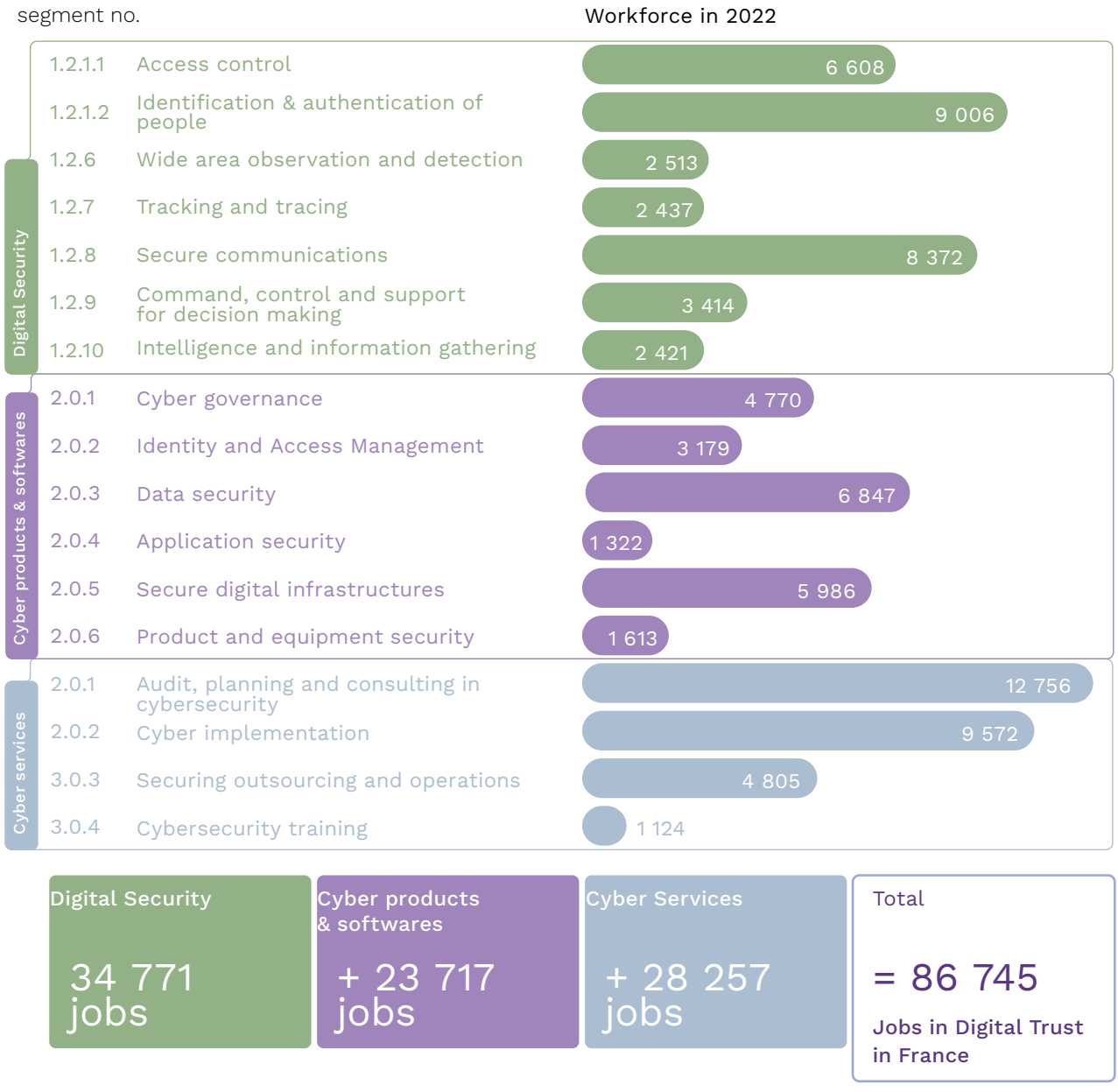
Added value in France in 2022 per segment



Source : Decision Etudes & conseils

3.3 Workforce

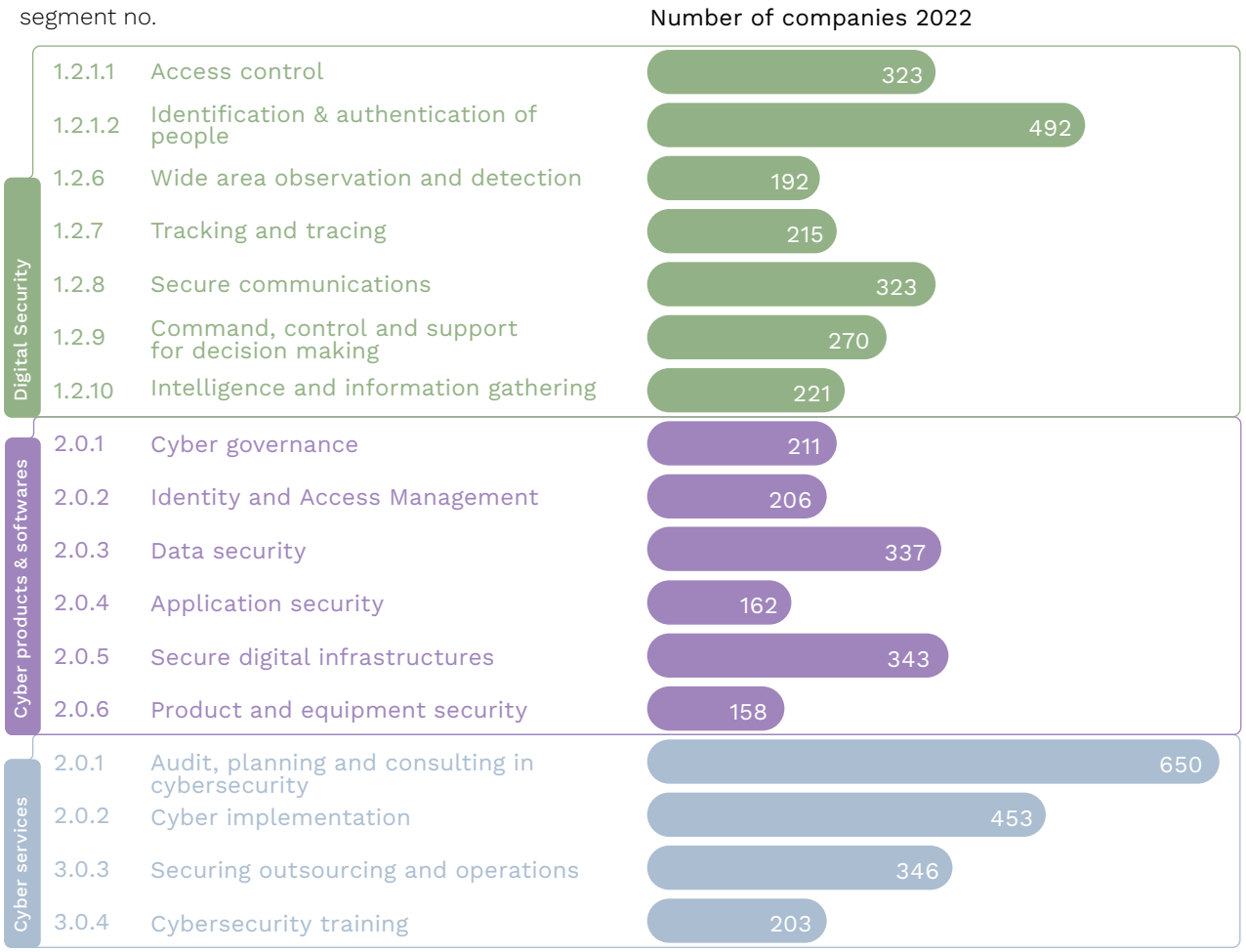
Workforcer in France in 2022 per segment



Source : Decision Etudes & conseils

3.4 Number of companies

Number of companies in france in 2022 per segment

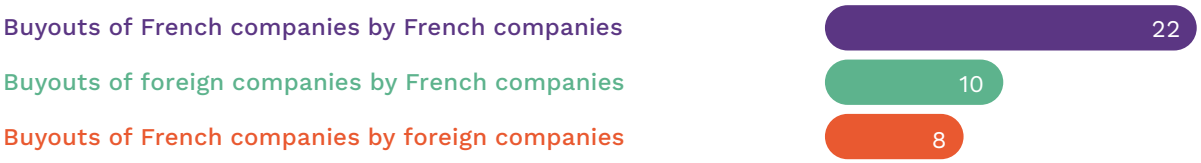


Digital Security	Cyber products & softwares	Cyber services	Total
1 741 companies	+ 703 companies	+ 690 companies	= 2 129 Companies in Digital Trust in France

Source : Decision Etudes & conseils

3.5 Mergers and Acquisitions

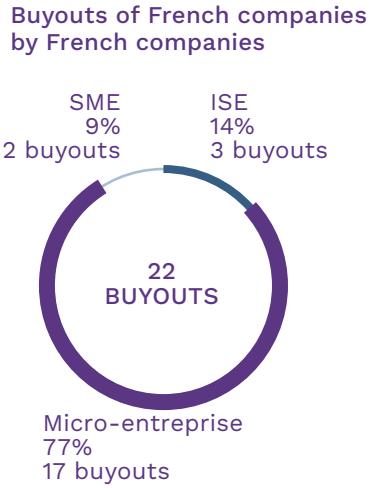
Company buyouts over the 2021-2023 period



Within the Digital Trust industry, **41 company buyouts** concerning headquarters located in France have been identified from January 2021 to March 2023 (i.e. an average of 17 buyouts per year). These buyouts are both inter-company purchases and purchases of companies by financial funds and purchases between financial funds.

Among them:

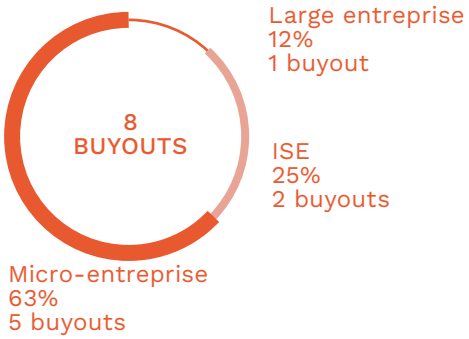
22 buyouts of French companies by other French companies (54%)



Source : Decision Etudes & conseils

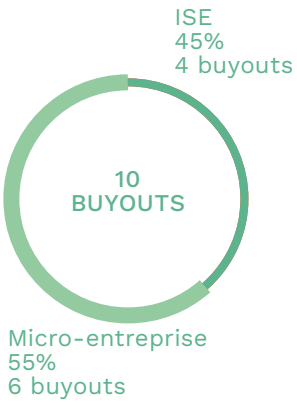
8 buyouts of French companies by foreign companies
(19%)

Buyouts of French companies by foreign companies



10 buyouts of foreign companies by French companies
(27%)

Buyouts of foreign companies by French companies



The vast majority of companies acquired are SMEs (68%) and ISEs (24%), which are growing.

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.**

In 2021, two-third of the buyouts of French companies by foreign companies were for the benefit of American capital, in line with the 2017-2020 period. These include Link by net, Openminded and AFD.TECH, all three of which were acquired by Accenture. **On the other hand, no buyouts of American companies have been identified in 2022.**

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. The main movements of Mergers and Acquisitions in 2022 in France

ChapsVision and its cybersecurity branch Flandrin Technologies.

French data analytics software company ChapsVision has grown rapidly in recent years, with the aim of becoming a leading player in the field of massive data processing. Since 2021, ChapsVision has made several strategic acquisitions in the cybersecurity sector, strengthening its market position and significantly expanding its activities. Among ChapsVision's latest acquisitions:

■ In 2021, acquisition of Bertin IT and Vecsys from CNIM, two companies specialized in cyber intelligence, business intelligence, automatic speech processing and cybersecurity software solutions. Thanks to these acquisitions, ChapsVision plans to increase its revenue from 30 to more than 40 million euros and its workforce from 260 to 380 employees. This double operation is part of the group's strategy to capitalise on data protection.

■ Late December 2021, acquisition of Elektron, a subsidiary of Nexa Technologies (historical partner of the Ministry of Justice, providing judicial interception solutions). Following this acquisition, ChapsVision creates its branch dedicated to cyber activities, named Flandrin Technologies. The objective is to create a sovereign player and European leader in this field. Flandrin Technologies now includes Bertin IT, Vecsys and Elektron.

■ Late 2022, acquisition of Deveryware, financed by a €100 million fundraising, led by Bpifrance and Tikehau Ace Capital. Deveryware is a leader in investigation technologies and services for global security. The objective of this acquisition is to consolidate ChapsVision's position in cybersecurity and investigative technologies, while offering services to public departments. Deveryware will become part of Flandrin Technologies, bringing the group's revenue to €100 million and its workforce to 500 employees.

These acquisitions are the most notable examples of the 10 buyouts ChapsVision has made in the cybersecurity sector since its inception in 2019. The company's goal via its Flandrin Technologies branch is to achieve €250 million in revenue by 2024.

Thanks to a targeted and ambitious acquisition strategy, ChapsVision is on its way to becoming a major player in the cyber sector. The group continues to strengthen its market position and consolidate its expertise in cybersecurity and massive data processing technologies. This rapid growth illustrates ChapsVision's ability to adapt to the challenges of the industry and to meet the growing need for data protection and cyber security.

Sopra Steria acquires CS Group for €283 million and becomes the number 5 in the industry in France.

Sopra Steria, the European leader in digital services and software publishing, has announced the acquisition of 75% of the share capital of CS Group, a specialist in critical systems and cyber security. This strategic acquisition aims to position the two companies as new champions in cybersecurity.

The acquisition of CS Group will allow Sopra Steria to strengthen its position in the cybersecurity market and benefit from significant synergies in terms of technical and business expertise in order to better respond to the challenges of security and digital trust faced by companies and public organisations.

Docaposte acquires Idemia's electronic signature and digital safe activities.

In early 2022, Docaposte acquired the electronic signature and secure storage businesses of Idemia, a leading player in digital identity and biometrics. The value of the acquired business is estimated to be €57 million and will enable Docaposte to consolidate its position as France's number one electronic signature provider by adding a new digital storage technology brick to its range of trust solutions for regulated markets.

B. The main movements of Mergers and Acquisitions in 2022 in Europe

Thales acquires S21sec and Excellium from Portuguese multinational company Sonae Group for €120 million.

S21sec and Excellium are two major players in cybersecurity consulting, integration and managed services in Europe. With this acquisition, Thales accelerates the execution of its cybersecurity roadmap and strengthens its presence in Spain, Portugal, Luxembourg and Belgium. S21sec and Excellium employ a total of 546 people and will have combined revenues of €59 million in 2021. This acquisition completes Thales' cybersecurity portfolio, strengthening its incident detection and response services (Security Operations Centre - SOC) as well as its consulting, audit and integration services. Orange Cyberdefense acquires Swiss companies SCRT and Telsys. SCRT is a company specialised in auditing and penetration test, SOC, consulting and solutions integration, while Telsys, founded in 1989, is a company positioned in the network infrastructure, cloud and datacenter sectors. Thanks to this double acquisition, Orange strengthens its expertise in threat intelligence and ethical hacking. The financial amounts of the transactional are confidential.

Sopra Steria acquires Tobania, a Belgian digital services specialist.

In November 2022, Sopra Steria announced the acquisition of the digital consulting and services company Tobania. Created in 2014 following the merger of two companies, Saga Consulting and Tobius, this Belgian company has 650 employees and revenue of €110 million.

Airbus strengthens its cryptography capabilities and enhances the development of end-to-end secure systems.

DSI Datensicherheit GmbH (DSI DS) is a German-based company that provides cryptography and communication systems for Space, Airborne and Naval & Ground that is certified by the Federal Office for Information Security (BSI). The acquisition follows a longstanding partnership between the two companies. DSI DS will be fully owned by the Airbus Defense and Space GmbH and operate under a new name, Aerospace Data Security GmbH. This will further strengthen Airbus' cryptography capabilities and enhance the development of end-to-end secured systems.

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 start-ups has **grown exponentially over the past 5 years.**

As shown in the infographic below, 21 fundraisings took place in 2020, 28 in 2021, 39 in 2022 and 6 in the first three months of 2023, already exceeding the amount raised in 2020.

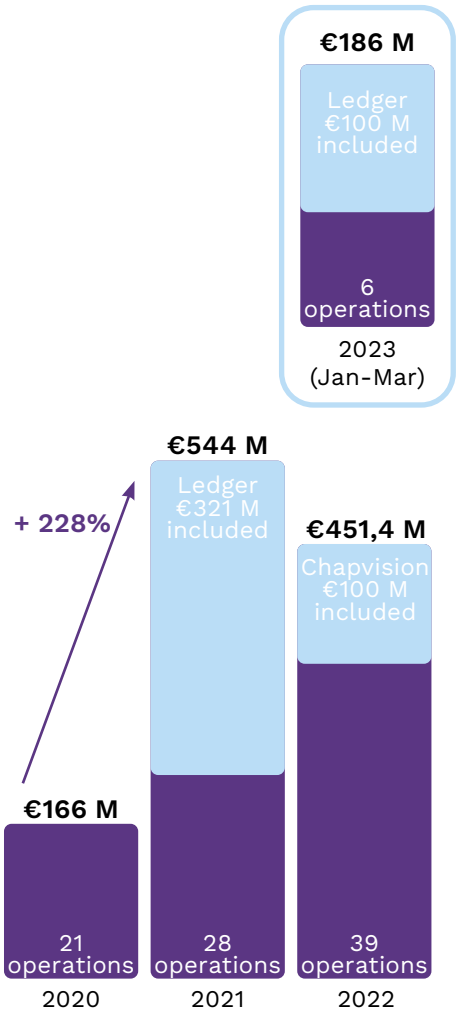
The sector has seen three exceptional fundraising rounds in three years: €321 million for Ledger in 2021, €100 million for Chapsvision in 2022 (used in particular for the acquisition of Deveryware), and again Ledger with €100 million in March 2023. Excluding these oneoffs, fundraising **amounts have continued to grow, reaching in 2022 more than double the amount in 2020.**

Of the fundraising recorded in 2022, out of a total amount of €351.4 million, excluding ChapsVision, ACN members account for 40% of investments, i.e. €140 million. Among the main French players behind these fundraisings are the BPI, Tikehau Ace Capital, Jolt Capital, Elaia, Move Capital, Alliance entreprendre, Seventure Partners, etc.

France is one of the leading countries in Europe in terms of fundraising for digital trust: **second in terms of the number of funds raised and third in terms of the amount raised.** This position is all the more significant for the sector and for France since, according to the European cybersecurity investment barometer carried out in 2023 by Tikehau Ace Capital, Europe will see a drop in fundraising across all sectors between 2021 and 2022, while cybersecurity, despite a slight drop in the number of funds raised, confirms its growth in terms of amounts raised.

According to the same barometer, although the majority of the world's largest fundraising is still in North America, Switzerland is recording a record year with two fundraisings appearing in the top 12 largest in 2022. At the same time, the average amount raised in the US is decreasing, while Europe is consolidating its 2021 growth (with a 39% decrease in the US and a 34% increase in Europe).

Amount of funds raised by French Digital Trust startups



List of fundraising activities of French Digital Trust startups

In 2021

	Company	Organisation	Year	Amount (€ million)
1	Ledger		2021	321
2	uitGuardian		2021	39
3	atadome		2021	30
4	ousign		2021	30
5	Didomi		2021	29
6	esWeHack	ACN	2021	16
7	r0ph3cy	ACN	2021	15
8	limps	ACN	2021	6
9	Zama	ACN	2021	6
10	Harfanglab		2021	5
11	Sis ID		2021	5
12	Ubble	ACN	2021	4
13	Crowdsec	ACN	2021	4
14	Cryptosense		2021	3,9
15	Artifakt		2021	3,7
16	Astrachain		2021	2
17	Anozr Way	ACN	2021	2
18	Data Legal Drive		2021	2
19	Eho . link		2021	2
20	Digeiz	ACN	2021	1,7
21	Mantra		2021	1,6
22	NanoCorp	ACN	2021	1,6
23	Qiova		2021	1,3
24	Altrnativ	ACN	2021	1
25	CryptR	ACN	2021	0,6
26	Mi-Trust		2021	0,5
27	Qontrol	ACN	2021	0,5

In 2022

	Company	Organisation	Year	Amount (€ million)
1	ChapsVision		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	ACN	2022	1,2
33	Kubo Labs		2022	1
34	Dastra		2022	1
35	Legapass	ACN	2022	1
36	Cyberjobs		2022	0,9
37	dappy		2022	0,5
38	Ravel		2022	
39	Eyst		2022	

In 2023

	Company	Organisation	Year	Amount (€ million)
1	Ledger		2023	100
2	DataDome		2023	42
3	Egerie		2023	30
4	Sesame IT		2023	10
5	Dotfile		2023	2,5
6	Defants		2023	2
7	Alcyconie		2023	2

3.7 The emergence of a strong ecosystem of Digital Trust SMEs

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 €15.3 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 €50 million 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 and €2.5 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).

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

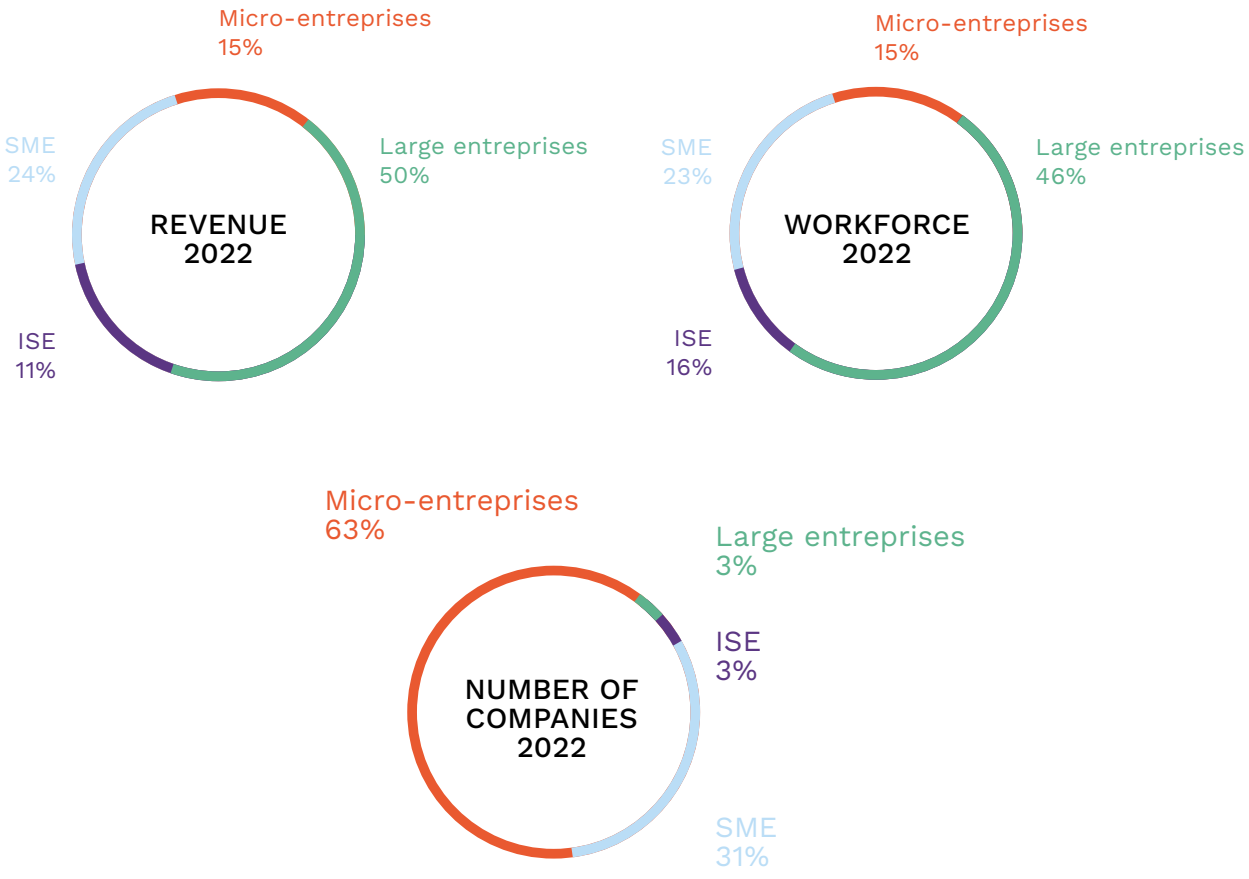
Emergence of a strong ecosystem of SMEs

€2,5 to €3 Billion in 2022

Major Historical Players

€15.3 Billion in 2022

Analysis by size of entreprises



IV. CURRENT STATUS OF ONLINE THREATS

4.1 Threats from the ANSSI's point of view

In its Panorama of Cyber Threats 2022, the ANSSI (French network and information security agency) reviews the major trends observed in 2021-2022 and proposes short-term evolution perspectives.

With an overall level that remains high, the ANSSI notes that this threat decreasingly affects regulated operators and is shifting to less well-protected entities. While the number of ransomware attacks reported to the ANSSI has decreased, the threat of spyware remains significant, having strongly mobilized the agency's teams once again.

Evolution :
23.2% decrease in proven intrusions

2021 :
1,082 proven intrusions

2022 :
831 proven intrusions

Note: While the number of proven intrusions is on the decline, the consequences of cyberattacks over the 2021-2022 period remain as serious or even more significant

Reference:
Panorama de la Cybermenace 2022
ANSSI - February 10, 2023

Document available below (in French):
https://www.ssi.gouv.fr/publication/un-niveau-eleve-de-cybermenaces-en-2022/

1. An overall threat level that remains high, notably for those with lower protection

The cyber threat has not seen any major changes, as **the trends identified in 2021 were confirmed in 2022**. However, although the number of proven intrusions is decreasing, the consequences of cyberattacks over the 2021-2022 period are just as serious or even more significant.

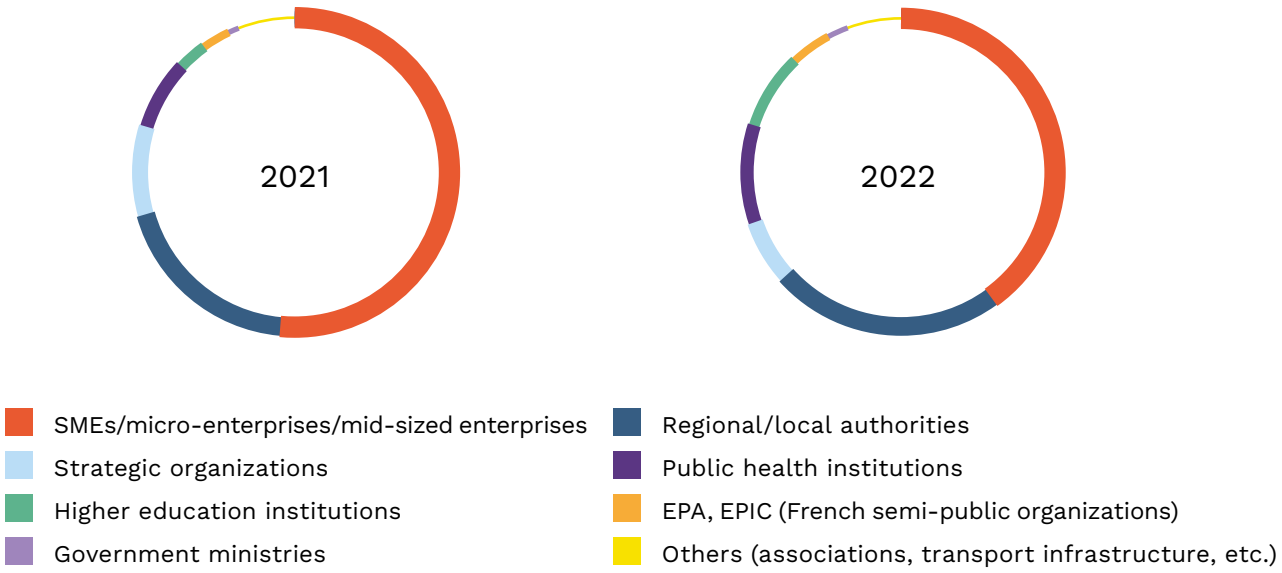
The ANSSI specified that at the beginning of 2022, the number of proven intrusions fell by 46% but that they **intensified once more in the summer of 2022**, particularly with regard to local and regional authorities and public health institutions.

In addition, the conflict between Russia and Ukraine has redefined the cybercrime ecosystem, with some Russian-speaking groups, such as Conti, shifting their targets to align themselves with Russian interests in Ukraine. Conversely, some cybercriminals are targeting Russia while others remain focused on purely lucrative attacks.

Private offensive cyberwarfare organizations offering spyware also remain highly active.

The graphs below show the evolution of ransomware targets as part of the incidents handled by the ANSSI in 2021 and 2022, ransomware having been the most common cyberattack over this period:

Types of ransomware compromise victims



As a result, the attacks decreasingly affect regulated operators and are shifting to the least protected players such as SMEs/micro-enterprises/mid-sized enterprises, local authorities and public health institutions.

2. Continued improvement in malicious actors' capabilities with the same objectives as 2021

The ever-improving capabilities of malicious actors observed by the ANSSI can be seen in their increasingly discreet and permanent access to their victims' networks. To achieve their objectives, malicious actors jeopardize peripheral devices (firewalls, routers, etc.) as well as the entire supply chain (service providers, suppliers, subcontractors, regulatory bodies, etc.).

Hackers' main objectives remain, as in 2021, financial gain, espionage and destabilization. The ransomware attacks on the **governments of Montenegro** in August 2022, as well as Peru and **Costa Rica** in April 2022, are significant examples of attempts at destabilization. As a result, they have had serious consequences on the running of these countries' governments and digital public services. Indeed, Cuba declared a state of emergency right after the attack.

In France, computer espionage was what mobilized ANSSI teams the most, and as in 2021, **the majority of cases handled involved operating modes associated with sources accessible by China**. During the first half of 2022, the ANSSI dealt with the compromise of a defense sector information system of potential interest to foreign governments.

The Russian-Ukrainian conflict has given rise to numerous acts of destabilization and espionage through network sabotage attempts on critical infrastructures, **but remain within the geographical limits of Ukraine**. However, the evolution of the conflict and the resulting economic consequences call for vigilance on the part of all organizations, particularly in the energy sector.

In Europe and North America, destabilization has taken the form of website defacement or informational operations by data exfiltration and has left numerous victims in its wake. **A resurgence of hacktivism has also been observed in 2022**. Nonetheless, media coverage of counter-measures was often disproportionate to the skill level deployed and the real impact on targets' operations. The consequences were confined to the unavailability of certain resources and damage to the image of the targets.

3. A threat that is difficult to determine with new operating modes

The increased complexity of malicious activity mapping is due to the use of operating modes assigned in 2022 to stakeholders different from those in 2021. **The use of ransomware is now not only attributed to cybercriminals, but to state actors as well**. For example, Albania has suffered several ransomware and wiper attacks (malicious programs aimed at destroying data on an information system) as part of a destabilization operation, which led to the temporary unavailability of several digital services and government websites.

Likewise, new malware is being used for cybercrime and espionage. This is the case, for example, with the DarkCrystal RAT modular backdoor, offered for sale on Russian-speaking forums, and which consists of a stealer (malicious program that collects various types of information before transmitting it to its operator) that adapts to the attacker's objectives by adding keystroke logging modules, collecting credentials saved on the web browser, and taking screenshots.

The main means identified by the ANSSI for the 2021-2022 period are the following:

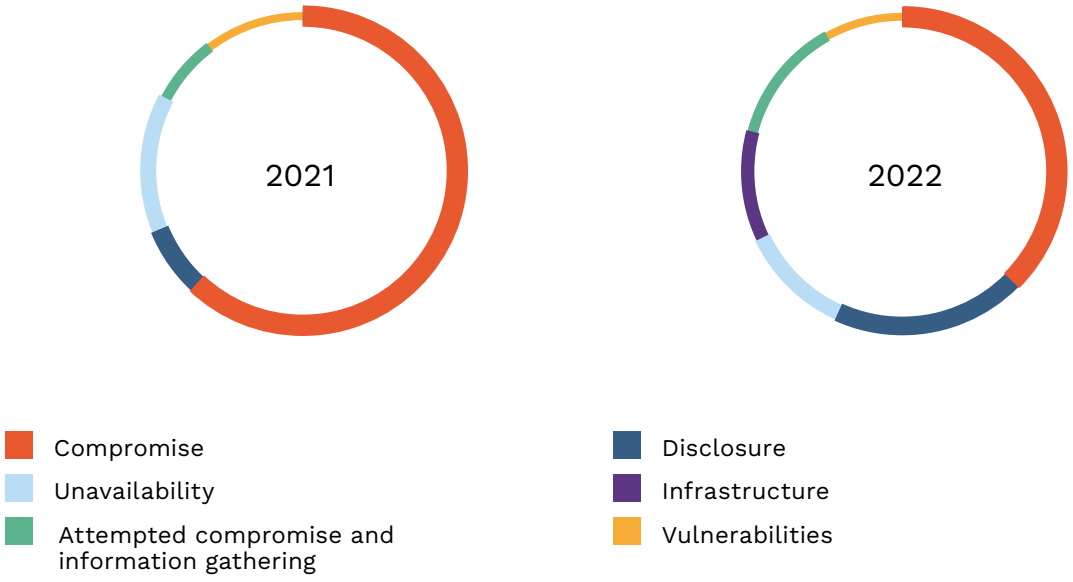
- Distributed denial of service (DDoS) attacks;
- Ransomware attacks by groups such as Avaddon, Bitlocker, Black Cat, Conti, Darkside, Everest, Hive, LockBit, Mespinoza/Pyza, Phobos, Play, Ryk and Sodinokibi;
- Health insurance scams;
- Reselling data for credible phishing campaigns;
- Services that sell user access or malware.

Cryptomining is also used to raise significant funds that malicious actors reinvest to acquire new capabilities. This tactic has become increasingly harder or impossible to detect as attackers manage to consume less computing power on compromised machines or flawlessly hide their tracks. Cloud infrastructures can be exploited for cryptomining purposes.

In the same way, many incidents observed by the ANSSI over 2022 **were caused by the exploitation of vulnerabilities which features patches and have been the subject of advisories or alerts on the CERT-FR website.**

In 2022, nearly half of the cyber defense operations and major incidents handled by the agency involved new operating modes associated with open source in China. This is because new technologies, new uses, cloud computing (a provision of IT services over the Internet) and outsourcing of IT services have broadened the attack surface.

Types of incidents impacting Digital Service Entreprises comparison



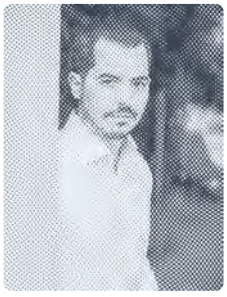
4.2 Perspectives from industry experts

Revolution in ID theft

Erwan Keraudy
CEO

«Hacked e-mails were the leading cause of data leaks and cyberattacks in 2022, and new compromised credentials are increasing by 45% annually. Infostealer malware is gaining significant momentum. Downloaded without users' knowledge, these spyware programs infiltrate computers and exfiltrate with utmost discretion sensitive information such as privileged access to computer networks as well as confidential and personal data. Cybersecurity startup CybelAngel detects over 20 million compromised credentials every week. The threat will continue to grow and weigh on the cyber landscape in 2023, so it is crucial for security measures to be taken now.»

Protect your infrastructure from USB threats



Quentin Ruillere
Co-founder & CEO

«USB keys that introduce malware into an organization's information system are unfortunately the most classic cyberattack. Between usbKiller, rookit or backdoor keys, 30% of infections originate from USB media and 40% of USB keys contain at least one file that presents risks. While employee awareness of such risks is essential for them to know what to do next, it is still not enough. According to the ANSSI, only air-gapped workstations can prevent any risk of infection. These are stations dedicated to analyzing and managing USB devices (regardless of whether they are USB keys, removable hard drives or DVD drives). Hogo is proud to offer the only ANSSI-certified (CSPN level) air-gapped workstation on the market.»

Toward secure and sovereign data ecosystems

Julia Chaulet
CEO & co-founder

«The limits of outsourcing data storage and processing have started to show. Cloud computing giants are far from immune to cyber risk and every one of their failures costs their customers dearly: the numerous data disclosures from AWS servers are a direct illustration. The French government and French organizations are stepping up their efforts to wean themselves off of their technological dependence on American giants. Initiatives such as the SecNumCloud security visa or the France 2030 plan promote French initiatives and innovations to meet this challenge. In this context, secure and sovereign data sharing technologies must expand to guarantee the growth of French and European organizations.»

The invisible threat of hybrid networks

Fanch Francis
CEO

«Hybrid networks (on-premise and cloud, IT and OT, or core and edge) have grown exponentially, multiplying the cybersecurity challenges along with them. Monitoring all networks from a single point of view is essential to ensuring comprehensive protection. NANO Corp offers a unified platform to detect and respond to cyber threats on such networks. Machine learning algorithms and behavioral analysis enable accurate anomaly detection and automated incident response. This solution is necessary for both SOCs and NOCs. It allows them to maintain control over their attack surface by taking into account undeclared, orphan or unmanageable machines, thus minimizing the risks of costly data breaches and reputational damage.»

More widespread adoption of strong authentication

Bruno Bernard
Chairman

«Digital data security is the essential shield against cyber threats coming from more directions than ever. In 2022, over 51 types of threats were managed by the cybermalveillance.gouv.fr platform, with phishing at the top of the list. To counter such increasingly sophisticated attacks, two-factor authentication via SMS no longer suffices. For maximum security, strong authentication methods are recommended, such as FIDO hardware devices. The FIDO standard has been adopted by Microsoft, Google, Apple and more than 150 service providers including identity federations such as Evidian, Ilex, Systancia, Octka, Ping Identity to name a few.»

The need for greater maturity in the smallest entities to effectively address cyber threats

François Esnol-Feugeas
CEO

«No matter how much ransomware threats seem to be on the decline, they remain the number one risk for organizations, and continue to make the headlines - the Centre Hospitalier Sud Francilien or the Grand Est Region being just a few of many examples! This threat particularly affects smaller entities, which have less experience in cyber risk management. The need to increase the level of protection in these structures is therefore critical, given the fatal risk they run when no disaster recovery plan (DRP) exists. The need for easy-to-deploy and affordable cybersecurity solutions, both technically and financially, has never been greater. »

A protean threat that continues to hone itself

François Deruty
Chief Intelligence Officer

«2022, the year of cyberwarfare? Definitely not: despite a spike in cyber activity in the region, the war in Ukraine has not had the desired effect in cyberspace. But while we're looking at the Russian side, Chinese-speaking APT actors are taking a more offensive approach in strategic and economic espionage... and targeting France. 2022 was also the year in which infostealers - programs aimed at stealing personal data - went professional. Similarly to ransomware, the cybercrime ecosystem has become structured and the «as-a-service» market has expanded. These developments confirm the need for organizations to have effective detection capabilities, thanks to accurate intelligence on hackers and their modus operandi.»

SMEs and micro-enterprises: Action speaks louder than awareness alone

Léo Richer
CEO

«The leaders of SMEs and micro-enterprises are well aware of the cybersecurity risks that their organizations are up against. However, many choose to ignore the problem, believing that the right solutions would be too expensive or complex to implement. It is up to the industry to convince them that the right solutions exist. To do so, it is essential to make them aware of their current situation and inform them of their options, while proposing solutions and adapted areas for improvement. The ANSSI has set the pace by advocating the need to mass-enforce cybersecurity. It is now time to normalize this approach and ensure that small businesses are not left behind.»

Our perception of the threat summarized in 3 V's: Velocity, Volume, Variety

Laurent Oudot
CTO

«In recent months we have analyzed millions of threats in more than 120 countries. The following trends were identified:
- Ransomware is still the main threat, accompanied by double extortion (disclosure of sensitive data if ransoms are not paid up) despite a slowdown at the beginning of the war in Ukraine that forced cybercrime groups to re-organize (for or against Russia)
- Phishing via e-mail, SMS and mobile applications remain the primary means of obtaining sensitive information
- Supply chain and IoT attacks have increased
-The most devastating operations used vulnerabilities in Microsoft products (Windows, Office, Exchange, Active Directory) or other applications that were sometimes too exposed.

Cyber defenders are very good, but their allocated resources are sometimes not sufficient to face of current threats.»

Bruno Charrat
Deputy director of technological research, CEA

Jean-Yves Marion
Director of the Lorraine laboratory for research in computer science and its applications (LORIA)

Scientific consultant for the CNRS cybersecurity department

French research mobilized to thwart cyber threats

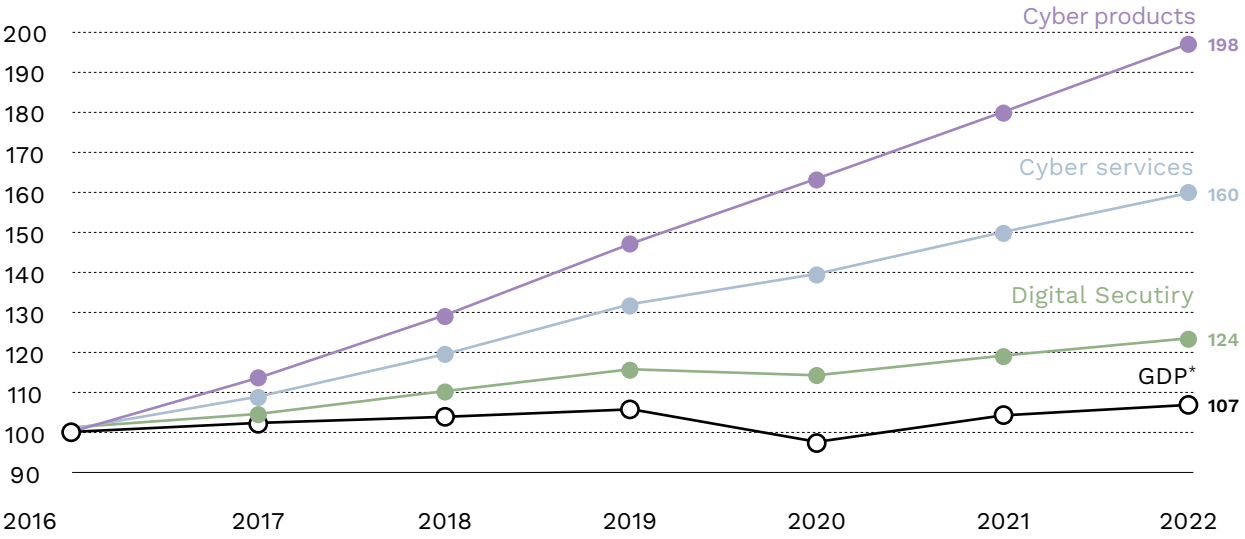
«Faced with a rapidly evolving cyber threat, it is more essential than ever to contribute to control over sovereign and secure digital technologies. France has a research community of excellence in cybersecurity. The national strategy for cybersecurity mobilizes it in collaborative and cooperative approaches with socio-economic and state actors on the entire continuum of fundamental research, innovation and entrepreneurship. Its research program (PEPR) aims to provide answers to ten fundamental research challenges. The Cyber Campus Transfer Program (PTCC), more focused on applied research and technology transfer, also supports training and entrepreneurship. These new tools allow us to structure interdisciplinary research communities at the highest world level to develop the technologies and tools that are essential to the sector and to contribute to a secure and resilient digital transition for citizens, companies and institutions.»

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 2017-2022



	Growth					
Segments	**2017**	**2018**	**2019**	**2020**	**2021**	**2022**
Digital Trust	**7,8 %**	**8,2 %**	**8,5 %**	**3,6 %**	**7,3 %**	**10,1 %**
Cyber products	14,3 %	13,9 %	14,0 %	10,9 %	8,8 %	10,5 %
Cyber services	9,3 %	9,9 %	10,3 %	5,8 %	8,9 %	10,7 %
Digital Secutiry	4,2 %	4,7 %	4,8 %	-1,7 %	5,2 %	9,4 %
GDP*	1,1 %	2,3 %	1,9 %	1,8 %	-7, %	6,8 %

*Source: INSEE, FMI for 2022

5.1.a. The growth of the French sector

2021 : A strong post-COVID recovery

In 2021, after a year marked by the COVID crisis, the Digital Trust sector has returned to strong growth of 7.2%, driven by structural trends that emerged more than ten years ago and are increasing year on year.

Key drivers for the Digital Trust growth

■ **Accelerated « digital » growth** driven by the health crisis and increased connectivity needs. Teleworking has increased the attention of companies on cyber security issues (secure teleworking platforms, etc.), as well as the importance of digital payments that need to be secure.

■ **Accelerated deployment of cloud platform** for companies but also cloud applications (Continuum Cloud-to- Edge), supporting the demand for a set of digital trust offers around trusted clouds, cloud security and at-the-edge security. These trends are particularly benefiting cyber product offerings: identity and access management (IAM), data security, infrastructure security, and product and equipment security (secure elements...).

■ **Continued increase in cyber attacks** (especially ransomware for several years). In addition, 75% of ransomware victims are now small and medium-sized businesses that lack dedicated resources (Orange Cyber Security Report, 2021). The market for the protection of French SMEs and VSEs is therefore very promising. In 2023, the Orange Security Navigator Report notes, however, a slowdown in the growth of cyber attacks for the first time.

The downward trend in cybersecurity growth

Since 2018, there has been a downward trend in the growth of the cybersecurity sector. This is simply due to the fact that **the sector is starting to reach a significant size with almost €10 billion being generated from France in 2022**. Growth is therefore continuing, but the growth rates relative to the size of the sector will gradually fall below the 10% mark. A sign of the very strong growth of this segment, **the revenue generated in France by cyber products has doubled in 6 years (between 2016 and 2022).**

Particularly strong growth in 2022, driven by digital security

The year 2022 is marked by particularly strong growth. Cybersecurity has a good year with 10.6%, slightly below the trend of the years 2014-2019. However, digital security had an exceptional year with a growth of 9.4%. This growth has three explanatory factors:

The subsistence of 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 pass-through of higher semiconductor prices following the global shortage, leading to value growth. This is particularly true for the personal identification and authentication segment (smart cards, etc.) and for the cyber segment of equipment security (secure elements, HSM), but this phenomenon extends to all digital security.

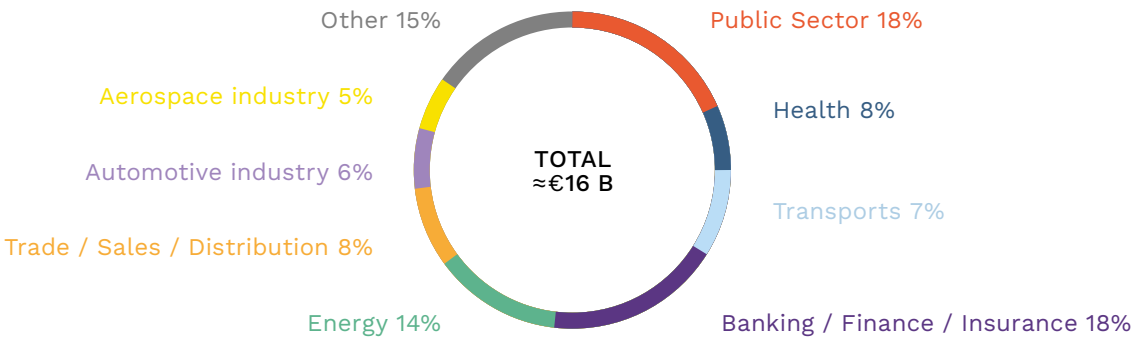
Lastly, a favourable economic climate leading to growth in volume: the growing importance of border control with increasing public projects, increased security demand from European states in connection with the war in Ukraine, security for major events (Rugby World Cup in France in 2023, Paris Olympic and Paralympic Games in 2024, etc.).

5.1.b. Markets in the industry in 2022

As shown in this diagram, the **public sector in the broad sense** - i.e. including transport and health - **corresponds to one third of the French market** (€5-6 billion in 2022), **with the remaining two thirds coming from the private sector** (€10-11 billion).

The weight of the private sector is set to grow year on year. The Digital Trust industry was born around the State and the need to secure Operators of Vital Importance (OIVs). The need for trust then extended to large companies in general, beyond the OIVs. The current trend is to develop the market for SMEs and Micro-entreprises, which are mostly powerless in the face of the risk of cyberattacks that now concern them, particularly the risk of being subjected to ransomware.

Main markets for the industry in 2022



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

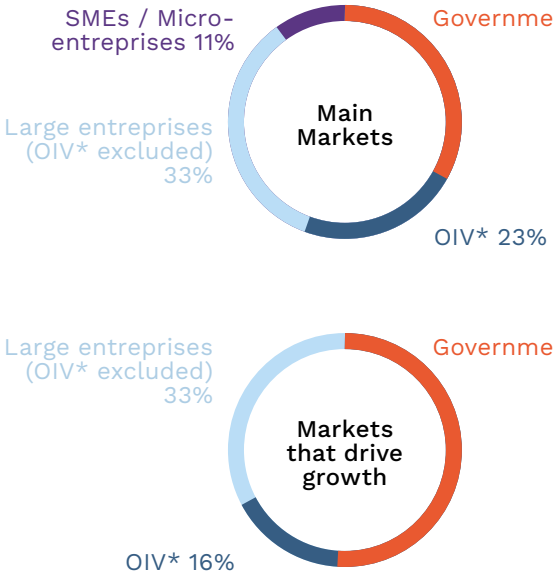
For the year 2022, the public sector continues to be indicated as one of the main drivers of growth by the companies in the sector that responded to our survey, along with the banking/finance/insurance sector and the energy sector.

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

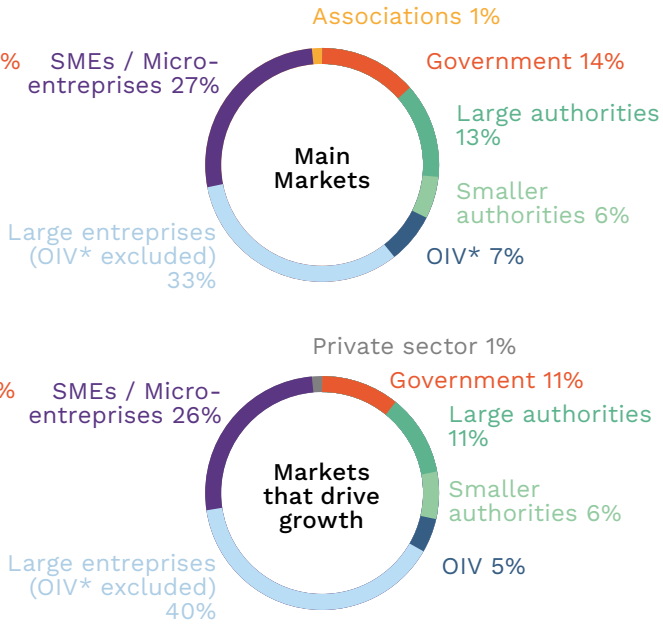
The series of diagrams below, taken from the 2023 edition of the online form sent to industry players, shows the segmentation of the French market according to the type of company providing trust solutions (large entreprises versus SMEs).

It can be seen that the State, the Operators of Vital Importance (OIV) and large entreprises (excluding OIV) account for almost 90% of the market for large enterprises in the sector (such as Thales or Idemia), and almost 100% of their growth prospects for the coming years. These large enterprises supplying trust solutions will account for 50% of the sector's revenue in France in 2022 (65% if activities outside France are included). We therefore find here the major traditional markets around which the sector has been built: the State, OIVs and major private accounts.

Large entreprises



Micro-entreprises / SMEs



* Essential operators identified by the government

In contrast, the State and the OIV only represent 21% of the market for SMEs and Micro-entreprises in the sector (such as Cyberwatch or Chambersign). Large enterprises (33%), Micro-entreprise/SMEs (27%) and local authorities (19%) 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 €800 million and €1 billion in 2022.

■ But most of all, **the development of the market associated with the need for trusted products and services on the part of French SMEs and Micro-entreprises.** By extrapolation, this market can be estimated at between 3.5 and 4.5 billion euros in 2022. 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.

Focus on Olympics - Securing the 2024 Games

TRIALS TO SECURE THE 2024 OLYMPIC GAMES: A COLLECTIVE SUCCESS THAT DEMONSTRATES THE DYNAMISM OF OUR INDUSTRY.

Gérard Lacroix
(GICAT), Deputy general delegate for security

Since April 2022, the Conseil Stratégique de Filière des Industries de Sécurité (CSF-IS) has been conducting a vast program of technological trials in cooperation with the ministry of the Interior and overseas territories, as part of an ambitious collective effort begun in 2018 to propose a global security plan for major events. Structured since mid-2019 around a group of leading names in the industry (Airbus, Atos, Idemia, Orange and Thales) materialized by the Global Security Proposal «Major Events and Olympic and Paralympic Games Paris 2024», the CSF-IS has led, through its innovative and original trial program, the success of a groundbreaking initiative. Under the leadership of Gérard Lacroix (GICAT) and Daniel Le Coguic (Atos), it brought together public authorities and industries around four main objectives: to guarantee the security and festive spirit of the Games, to substantially improve the capabilities of the internal security forces, to unite the French security industry and make it an international champion, and to contribute to the legacy of the Olympic program while developing an exportable model.

Focused on a series of key themes that are essential to French homeland security and emergency services, such as command centers, intelligence, cybersecurity, anti-drone technology, videoprotection, crowd management and CBRN defense, this program has enabled all players in the industry to be included, in particular SMEs and innovative start-ups. Widely publicized and open to all, through calls for expressions of interest (CEI), the approach has enabled the analysis of nearly 700 solutions from 171 different companies, thus demonstrating the wealth of the French industrial ecosystem. At the end of the CEI, close to 200 solutions were tested thanks to the involvement of 89 different companies. The results are unprecedented and go far beyond the objectives of inclusion and sovereignty initially set and taken by the CSF-IS, since 90% of the solutions tested were French (initial objective of 80%) and 75% of these solutions were from start-ups, SMEs or micro-enterprises (initial objective of 30%). GICAT members participated actively in 45% of the solutions trialled.

This tremendous investment by the industry is therefore a great collective success in the implementation of sovereign technologies and testifies to the dynamism of our industry.

As this phase of unprecedented mobilization in the French security industry draws to a close, the CSF-IS has drawn a number of conclusions from this program, which it has shared with the ministry of the Interior and overseas territories and the security forces. In this regard, substantial procurement plans in line with the ministry of the Interior's January 2023 Orientation and Programming Law (LOPMI) should be implemented with regard to command centers, cybersecurity, video protection, anti-drone technology, intelligence and intelligent border surveillance. In the perspective of the second industry contract, it now seems timely and relevant to extend this value-generating program to other components of the security continuum, to local authorities, to operators of vital importance and essential service operators. This approach could take the form of new trial programs, the creation of joint bodies (innovation laboratories) or, even more ambitiously, the structuring of export programs (Milan 2026, FIFA World Cup 2026, Los Angeles 2028, etc.).

What is LOPMI?

Eagerly awaited, French law no. 2023-22 of January 24, 2023 on the orientation and programming of the ministry of the Interior (LOPMI) sets out, for the next five years, the priority objectives in terms of public security policies, including the prevention of terrorism, the fight against drug trafficking and the repression of in-family violence. On the budget front, the law provides for 15 billion euro in additional funding. The Ministry of the Interior will thus be able to continue its upgrades, especially in the digital domain: dematerialized procedures, mobile work tools, modernized investigation means, etc. The reinforcement of the security continuum provided for by the LOPMI is a guarantee of the mobilization of all actors, both public and private, for the benefit of overall national security, particularly in view of the Olympic and Paralympic Games in Paris in 2024

History | The OPG2024 are exceptional in their size and duration

To illustrate the exceptional character of the event, a figure to remember: more than 12 million visitors from all over the world are expected to turn up. As an example, the Olympic Games (July 26 to August 11) can be compared to about 46 soccer World Cups. The Paralympic Games will take place from August 28th to September 8th.

Some key figures on this event:


12 million spectators


8 million fans at live sites


20 000 accredited journalists


17 000 athletes


70 000 volunteers


15 million people on the route of the flame


4 billion viewers


100 000 hours of TV broadcast


68 500 Security personnel

Source : PARIS2024 security technical annex / 2: With training sites etc (CNSJ)

Threats | The level of threats relating to the Rugby World Cup 2023 and the Olympic Games 2024 requires the ministry of the Interior to double down on its cybersecurity stance

The expected incident analysis related to cyberattacks will be extremely high and will peak during the 2024 Olympic Games. Attacks are likely to target mainly the Organizing Committee of the Olympic Games (OCOG), with the objective of disrupting but also by the lure of gain. Broadcast infrastructures of the Games, opening ceremony, physical and online communication means are some of the many threats that should be anticipated.

A threat level thriving in an exceptional context
The significant foot traffic before and during these events and live broadcasts will require a high level of vigilance, especially in a currently tense geopolitical context and virulent hacktivism (religious, ecological, etc.). France will indeed be the focus of the world during these few weeks.

Hacker profiles are diverse; there are those sponsored by foreign governments with unlimited means of attack to reach strategic targets, criminals motivated by ransom demands or hacktivists adept at website defacement, for example.

Issues | Security of major events in France represents challenges and opportunities for the industry

Securing the Olympic Games in 2024 is of strategic interest to France. It is an opportunity for success, to structure and enhance the value of our industrial sector. All stakeholders involved want to preserve the festive spirit of the games and give the public a significant role, while controlling costs and limiting the number of people involved. Through the constitution of an ecosystem integrating SMEs, micro-enterprises and startups, the entire security industry is being mobilized

This opportunity is justified by the possibility of seeing, at the end, numerous returns on investment. It accelerates the upgrade of current public security resources and the upskilling of private and public security personnel, while creating jobs for the industry. Accompanied by an evolution of the legal framework, initiating a controlled technological breakthrough, it will showcase France and the rich and diverse ecosystem that has been built around an industry of excellence that will promote the export of French know-how internationally.

CSF-IS | The strategic council of the security industry (CSF) is committed to the Ministry of the interior

Mixed Group

Steering Committee mixed

Report on the progress of the work and validate the areas of focus

Integration of AMI

Design Thinking Workshop

Refine risk analyses, requirements and the evolution of security systems

Taking into account the work of COFIS

Joint working groups and seminars

Evaluation of technologies and their impacts, feedback from security operators

Analysis of existing security plans

Between July and November 2019, the CSF-IS therefore worked in co-construction with the French government to draft ***four flagship documents***, meeting **four major objectives**:

1. Guarantee the security and festive spirit of the Games;
2. Substantially improve the capabilities of the internal security forces;
3. Unite the French security industry and make it an international champion;
4. Contribute to the legacy of the Olympic program and develop an exportable model.

Accompanying all phases of the project, these deliverables were **pillars of the architecture**, needs analysis and trial plan orientation phases.

Trials | The entire industry, the ministry of the Interior, ANSSI and SGDSN have joined forces through joint work: 192 trials to shed light on French expertise for ISPs

The trial program has been a rousing success, thanks to its innovative nature, which is the result of collaboration between the Ministry and organizations, and an efficient joining of forces. The **192 trials** have made it possible to **showcase French technologies** to security forces and **to test them in operational conditions**, as close as possible to their needs. The entire French industry is now committed to **supporting the modernization of the ISPs**, thus becoming part of a legacy approach.

The mobilization of the French industry was particularly evident in 2022, as part of the implementation of trials that enabled the development of solutions from ACN member companies: Anozr Way, Atos, Citalid, Egidium Technologies, Idemia, Orange, Owlint, Sahar, Thales, XXII, YesWeHack, and Yogosha.

The selection process was based on a widely publicized call for expressions of interest, which allowed **687 solutions** from **171 different companies** to be analyzed.

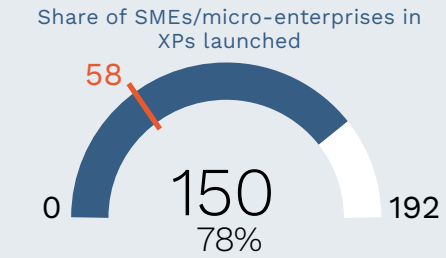
Component	No. of applicant organizations	No. of solutions analyzed	No. of participating organizations	No. of solutions trialled
Command & hypervision methods	59	195	30	52
Videoprotection	16	116	8	23
Cybersecurity	55	122	26	43
3D Bubble - Very Low Altitude	17	117	5	20
Other areas:				
Nautical	29	59	15	23
Crowd management & flow	17	29	12	17
NRBCE	17	49	10	14
GLOBAL	171	687	89	192

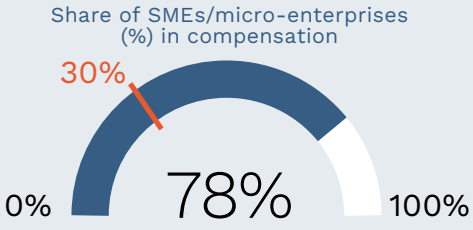
The trials have **made it possible to identify essential areas for technological reinforcement, thus improving the efficiency of the forces**. The approach implemented has made it possible to identify common needs, and voluntary action by the Ministry will make it possible to move on to the next stage by proposing :

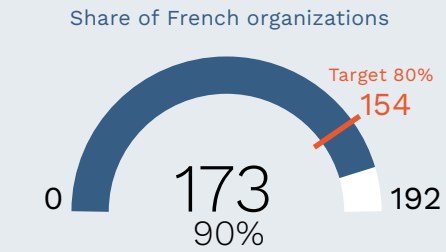
- The common purchasing pool;
- Standardization of technologies for the benefit of interoperability;
- The use of shared platforms.

This stage must materialize in acquisition plans for each of the trial components, the main two being **cybersecurity and command centers**:

- **16 cybersecurity projects co-constructed with the ministry of the Interior** with **3 deadlines**: the Rugby World Cup 2023, the Olympic Games 2024 and the LOPMI deadline 2027.
- 3 areas of upgrades relating to the convergence of command centers, and structuring the collection and restoration of their data.







Our future | Using the work initiated as a particle accelerator for the post-OPG2024 period

- **Capitalize on the approach**, crystallize ongoing initiatives, notably by enabling acquisitions of relevant technologies for ISPs, and make the JO project a particle accelerator for the entire industry and the modernization of the ministry.
- **Continue structuring** the industry mobilized around a brand team, joint communication actions and coordination with the various players.
- **Implement ongoing collaboration** with the Ministry of the interior through a **dedicated interface**.
- **Launch a coordinated and piloted program to export the French industry's know-how**.

Supporting the modernization of the security forces

Ensuring the security of the Paris 2024 Olympic Games

Structuring and developing the security industry sector through a major and mobilizing event

Building the legacy of the games

SECURITY OF THE 2024 OLYMPICS & PARALYMPICS GAMES SEEN BY THE MINISTRY OF INTERIOR

Olivier de Mazières

Ministerial Delegate for Partnerships, Strategies and Security Industries (DPSIS)

The Paris 2024 Olympic and Paralympic Games are currently the largest event organized in France, both in terms of size and duration. Ensuring the security of such an event is a major challenge. The evolution of threats, further accentuated by the widespread use of digital technology, requires the Ministry of the interior and overseas territories to constantly adapt its response.

This response does not only rely on the resources mobilized by the public authorities. It also requires the involvement of the individuals who make the global security continuum work, as well as organizations capable of providing the technical resources necessary to protect people and property.

This mobilization of stakeholders and technologies implies a fair assessment of needs, coordination of private and public actors and respect for a strict legal framework in terms of freedoms.

At the end of July 2021, the DPSIS was entrusted with the management of a security technology trial program to meet these challenges. It is a response to the French government's commitment in the security industry contract, co-signed in January 2020 by the Interior Minister.

In addition to the security of the Olympic Games and major events, it aimed to accelerate the transformation of talent, and to strengthen synergy with the industrial players united in the Comité Stratégique de Filière (CSF-IS). The aim was also to develop technological tools that are interoperable between various players, adapted to evolving threats and tested in real conditions with a view to possible acquisitions.

A budget of €21.5 million has been earmarked in the 2022 stimulus plan to organize these trials and compensate industry players.

The expression of needs mobilized the forces, the CNSJ, transport operators and several public stakeholders (SGDSN, DIJOP and DGTIM) on 7 priorities: command centers, cybersecurity, image processing, very low altitude security (including anti-drone warfare), NRBC-E, nautical security and flow management.

Out of the 192 solutions tested (out of nearly 700 proposed by manufacturers), 90% came from French companies and 77% from start-ups, SMEs and micro-enterprises.

The business units have already scheduled purchases for an estimated amount exceeding €60M, almost half of which will be purchased over 2023. Other acquisitions have yet to be quantified, notably in the areas of command centers, cybersecurity, border protection and intelligent video, with the implementation of the trial provided for by the recent law on the Olympic Games.

They have acted as a particles accelerator for the global security continuum. In addition to purchases, these trials have also enabled vendors to develop their products to better meet the needs of the forces, and for these forces to fully measure the availability, quality and density of sovereign solutions.

If this heritage seems dense, solid and relevant, it is first of all because it is empirical, based on permanent exchanges between the public and private sectors, designers, integrators and users. Real-life tests have enabled us to converge on solutions that meet the real needs and constraints of the field. It is a method that paves the way for future cooperation and outlines a model of ethical security for the major events to come, for the benefit of the protection of our citizens, the efficiency of our forces and the performance of our organizations.

The forthcoming creation of a Directorate of security and weapons organizations and partnerships (DEPSA) within the Ministry of the Interior and overseas territories, as well as the establishment of an R&D center, will boost this effort and strengthen this vital link between the forces and the security industry.

DPSIS

Délégation ministérielle
aux Partenariats, aux Stratégies
et aux Innovations de Sécurité

5.2 Regulatory trends

5.2.a. European regulatory landscape: towards a single trusted digital market

As the digital transition unfolds, the technologies developed have become indispensable to the daily lives of their users. These new uses lead to new risks that need to be controlled. In order to respond effectively to the resulting cross-border cyberattacks and to protect its fundamental values, **the European Union has set up an ambitious program called «For a Digital Europe», which aims to position the EU at the heart of this major challenge by 2030**. This program, which takes the form of numerous regulatory initiatives, addresses the EU's protection objectives in the face of digital risks (cybersecurity, cyber resilience, etc.), but also reflects the ambition to provide Europe with a leading digital economy, by regulating the digital market, stimulating the competitiveness of the players in the ecosystem as well as research and innovation in order to ensure European technological sovereignty.

Regulation of the digital market

As a first step, the European Union wanted to **protect the European digital market from illegal online content** (child pornography, terrorism, etc.) and products (counterfeiters, dangerous products, etc.) by harmonizing the national laws that already apply. The Digital Service Act (DSA) will apply to «very large platforms» (more than 45 million active users per month, i.e., 10% of the European population) as soon as the Commission designates them, and from February 17th, 2024 for the rest of the platforms.

As a second step, the Digital Market Act (DMA) protects European competition law from **possible unfair practices of «gatekeepers»** (sound, sustainable online platforms with a strong position providing an essential platform service) comes into force on May 2nd, 2023.

Protection of digital market players

The European Union wanted to **raise the common level of cybersecurity** across its territory to **guarantee a trusted cyberspace and strengthen cooperation between member states.** To this end, it has extended the scope of the NIS Directive to include new sectors that are essential and important to shoring up the economy and society in order to strengthen the cybersecurity of the entire supply chain. The NIS 2 Directive will take effect in October 2024.

ACN published its proposals for the French Presidency of the European Union in early 2022.

ACN Report
«French Presidency of the European Union European: ACN's proposals».
available for download on
www.confiance-numerique.fr

Building collective resilience

The Union has also undertaken to **limit the risks** posed by the **profound digital transformation of financial services and the increasing interconnection of networks and critical infrastructures.** The DORA regulation on the digital operational resilience of the financial sector, published on January 16th, 2023, will come into force on January 17th, 2025, harmonizing risk management in this sector.

Secondly, the draft Cyber Resilience Act (CRA), still under discussion, **will establish common cybersecurity requirements for all electronic and digital products placed on the internal European market.**

The Union now wishes to strengthen **cyber solidarity and crisis management capabilities** through the Cyber Solidarity Act announced on April 18th, 2023, backed by funding of €1.1B and which will be composed of three pillars: a **European Cyber Shield** (a network of national and cross-border SOC-Security Operations Centers), a **Cyber Emergency Mechanism** (including the creation of a European Cyber Reserve) and **a Cyber Incident Analysis Mechanism**. This system will be accompanied by a strengthening of skills in this area to address the cybersecurity **talent shortage** with the creation of a Cyber Skills Academy.

Lastly, digital identity and secure identification/ authentication of Europeans is also at the heart of regulatory developments with the ongoing revision of the eIDAS regulation. The eIDAS-2 regulation sets the European framework for a digital identity (electronic identification). The revised regulation aims **to ensure universal access for individuals and businesses to secure and reliable electronic identification and authentification through a personal digital wallet.**

The proposal will require Member States to issue a digital wallet under a notified electronic identification scheme, based on common technical standards (Architecture and Reference Framework - ARF) and after a mandatory compliance assessment.

Focus - Press viewpoint

TOO MANY RULES DAMAGE TRUST

Delphine Sabattier

Delphine Sabattier is a journalist, presenter and producer, specialized in France in innovation and digital policies.
She explores and popularizes the issues surrounding the transformation of society and ecosystems through press articles, her TV editorials on LCP, audiovisual productions, and her daily discovery and innovation program Smart Tech on the channel B SMART TV (https://www.bsmart.fr/emissions/smart-tech).
Previously, Delphine managed the most prestigious information media dedicated to new technologies (Science & Vie micro, 01net and others). Today, she is a key figure in the tech information world.

“I was there with my microphone, ready to pick up the European Commissioner Thierry Breton for a statement, an answer to the expectations on securing the digital space: I was not disappointed! The surprise speech he delivered to cybersecurity professionals gathered at FIC2023 in Lille in early April had everything to please his audience: «Cyber resilience can only become a European topic» «coordinating our efforts is essential,» he emphasized, rolling out Europe’s new defense doctrine and unveiling the European Cyber Shield project.

This «dome», explained Commissioner Breton, is based on four pillars: protect, detect, defend and deter. For this, we need advanced technologies, infrastructures, cooperation... and sanctions. The European Commission is therefore working hard to establish the new frameworks for compliance. These regulations are eagerly awaited to create the conditions for trust, but paradoxically they could work against our ecosystem.

Indeed, ignoring the impacts of the regulation on our European players would be a mistake. It would penalize our industry, weaken our strengths and thereby move us further away from the quest for sovereignty. However, being in control of technologies and data is essential for trust. Of course, everyone agrees intellectually on this point. «Digital and industrial sovereignty» are the watchwords in every political discourse. But in reality?

With every new rule comes the announcement of a new acrobatic compliance exercise - where the first parties to come under pressure are the European companies of the sector. Europe is their native market. The sanctions are applicable to them de facto, whereas formal notices to big tech are much more complex and take longer to arrive. As for the risk involved: the fine for a European company is often more difficult to accept.

Collateral damage must not be neglected

Do you remember the account by Olivier Magnan-Saurin, from Fidzup? On February 5, 2020, he wrote angrily, «The CNIL has killed us». His French company did not survive the enforcement of the GDPR. He recognizes the necessary progress that the regulation provides on personal data protection, but wonders, «How can we create European champions in this context if the application of our laws is more restrictive for companies on the old continent than for the rest of the world? How can we reclaim leadership in technology or data storage if we strengthen the positions of the Americans or the Chinese?"

These concerns are still valid for the executives I meet at Smart Tech, with the arrival of the Cyber Resilience Act and the French Secnumcloud. However, trust depends on Europe's ability to develop its own technologies on the domestic market. Today, «major» cyber threats are geopolitical threats. This is why the European Union must create the means to become a technological power in cybersecurity: support, consolidate and strengthen its ecosystem to protect its sovereignty.

What if we started to trust each other?

My opinion: to develop trust, yes, we need protective, binding rules that apply to everyone. But Europe must also learn to trust itself.

This includes in particular Member States learning to trust each other. This is the goal of the Cyber Solidarity Act, which is undoubtedly the most conciliatory text that the Commission will publish in the field of cybersecurity.

But Europe must also believe in the ability of its technological players to become superpowers. We have gems in cybersecurity and more broadly in tech! I regularly receive them on the set. It's a pity, because they can more easily capture international markets than the order books of the French government! They defend a European-style Small Business Act... and would like the Commission to remember the impact on its own ecosystem when drafting its regulations.

I second them here with the conviction that in order to stand together in the face of major threats, we should start trusting one another in Europe. Let's not stifle the innovation we have inside. Otherwise, who will hold our shields?

Edouard Jeanson, Vice Chairman of ACN, interviewed by Delphine Sabattier on Smart Tech on the creation of a «single digital market». Broadcast live on B Smart, February 21, 2022.

5.2.b. National cybersecurity initiatives

To meet the challenge of digital sovereignty, strategic autonomy and improved national resilience, the President of the Republic announced in February 2021 **the deployment of a national cybersecurity strategy.** The goals set are to triple the industry's revenue, double the number of jobs and bring out at least three unicorns by 2025. Various operations have been launched to achieve this goal, **including the ANSSI's courses** designed to raise the level of cybersecurity in France, which are part of the cybersecurity component of the French recovery plan. The challenge now is to significantly increase the resilience of all public and private players throughout the country, and in particular to improve the protection of the most vulnerable organizations, i.e. healthcare institutions, as well as SMEs and micro-enterprises.

Several initiatives have already been launched for this purpose by the Minister Delegate in charge of digital transition and telecommunications, Jean-Nöel Barrot; the Minister of the Interior and overseas territories, Gérald Darmanin; and the Minister of Health and Prevention, François Braun; **in order to strengthen the cybersecurity of healthcare institutions,** which have been particularly targeted by cyberattacks over the past two years.

Concerning the protection of SMEs and micro-enterprises, the French government has also undertaken to set up a cyber shield, with €25M in funding to support them in their cybersecurity approach. This shield will be composed of three parts: awareness, provision of a cyber self-diagnosis and a security system.

France has adopted a **Cyberscore**, which should come into force in October 2023, and which takes the form of **a display of the level of protection offered by the major digital platforms**, intended for the general public, both from the point of view of cybersecurity and the protection of personal data, as well as exposure to the extraterritorial application of foreign laws. A public consultation has been launched by the Direction Générale des Entreprises (DGE) in order to finalize this project, and ACN has responded to this consultation in order to convey the industry's messages on this Cyberscore project and its concrete implementation.

In addition, **the strategic committees of the industry, and in particular the CSF-IS, are continuing their work** to complement these public initiatives. The CSF-IS roadmap is currently being updated, with the aim of signing a sector contract in the summer of 2023, which will include work on the following priority areas: Border security, everyday security operations, healthcare system security, cybersecurity for SMEs, certification/ regulation, community security, digital identity, promotion, strategy, security for the 2024 Olympics, attractiveness and skills and ecological transition.

5.2.c. Defining the criteria for Trusted Artificial Intelligence

Artificial intelligence, in the sense of the European Commission's proposed AI Act, is defined as «software that is developed by means of one or more of the techniques and approaches [...] and that can, for a given set of human-defined objectives, generate results such as content, predictions, recommendations or decisions influencing the environments with which it interacts».

The role of AI keeps growing in the daily life of its users. Often put forward only for marketing purposes, this technology remains **largely unknown and is the subject of a large amount of misinformation,** even disinformation, which raises fears and numerous debates that contribute to slowing down its development.

Organizations in the digital trust sector consider that AI is a technological building block for our digital future, but also **that mastering it is an essential challenge for the national digital sovereignty and strategic autonomy.**

For all that, the public debate must take place on all the questions that AI and its different uses may raise. But this debate must be enlightened and based on the technical reality of AI, and it is up to the legislator to set the framework within which these solutions can be developed in full confidence and in the respect of all the fundamental values of our French and European societies.

This is why the ACN has developed a roadmap to define objective criteria (legal, technical and ethical) that could serve as references in order to define with precision and clarity what makes a trusted AI. This is the purpose of a white paper currently being drafted by its working group dedicated to trusted artificial intelligence. This white paper will present the various facets and uses of this value-added technology in order to streamline and clarify the public debate and propose criteria to distinguish trusted AI.

This white paper first addresses **the legal framework of AI and its limits.** AI is considered by the texts currently in force as a «new technology» that should be controlled by binding obligations enacted within a more global framework and not specific to AI.

This has led to **many inappropriate interpretations,** which are unsatisfactory when they slow down the development, in France and in Europe, of these technologies that are essential to our mastery of the digital world in the future. To remedy this, **it is now urgent that specific regulations for AI be designed and adapted to the numerous and diverse uses of this technology,** in order to allow actors in this field to develop these technologies in an appropriate framework. **The European Commission's AI Act proposal is welcome** for this purpose. The new AI framework should enable a trusted ecosystem to gain competitiveness and foster synergy in the industry. This framework under construction seems to be a solid basis for the creation of an international standard for trusted AI.

Beyond that, trust is also established in the technical domain. Concepts such as explicability, predictability, transparency, limitation of bias, and quality of learning bases must **find precise, verifiable and auditable technical variations.**

Trust is established through the social **acceptability and ethics of AI.** It must be developed in accordance with the core values of the European Union and predefined principles such as those of the European Ethical Charter for the Use of AI in Justice Systems and their Environment adopted on December 3-4, 2018. ACN chooses to focus its attention on **the principles of human primacy** so that humans are always at the heart of this technology and that it does not decide in isolation from human control, the need for performance to ensure that it is appropriate, necessary and proportionate and that this technology is environmentally acceptable. These principles must nevertheless be shared, as widely as possible, in the public debate in order to **create a consensus around this notion of trust, which is essential for the confident development of strategic technologies for our future.**

Focus ANSSI - Cybersecurity component of the France Recovery plan

Assessment of actions taken

As part of France Relance, a cybersecurity component has been set up, under the guidance of the ANSSI. This plan, which amounted to €176M over 2021-2022, has enabled the deployment of several measures, notably for **the benefit of local authorities, healthcare establishments and for the security of government systems and networks.**

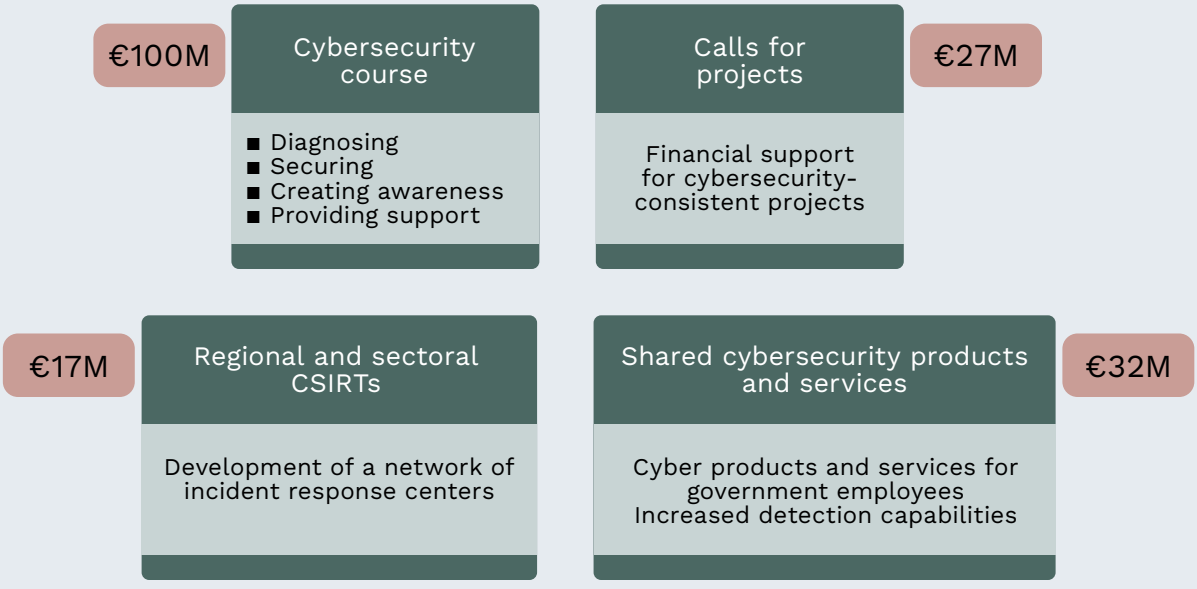
A win-win strategy at the heart of the actions:
Increase the cybersecurity of government and public services,
via the acquisition of products and services to strengthen the European offer

The overall results of this plan are extremely positive: it has led to a concrete increase in the level of cybersecurity among beneficiaries and to the widespread deployment of numerous solutions, most of which are European. The mobilization of the ecosystem of solution providers and publishers to meet the needs of users, as expressed through the proposed measures, has contributed to this success.

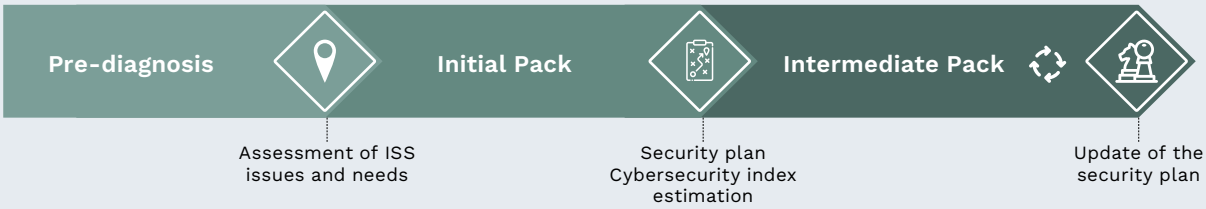
Actions taken

The schemes have focused on subsidizing the beneficiaries involved, with co-financing required. This mechanism offers the advantage of involving and empowering everyone in their cybersecurity projects, to help them identify and implement the necessary human, financial, administrative and technical resources.

A set of 4 major projects, all completed



The cybersecurity courses have helped 950 beneficiaries through a formalized approach thanks to concepts and guides previously produced by the ANSSI: digital hygiene guide or guide on ransomware attacks, as well as those with the support of the agency's experts who participated in the framing phase and in the definition of the courses. The design by ANSSI experts ensures the technical relevance of the system. Operational feedback has been taken into account to adapt it as closely as possible to needs. More than 170 field service providers are currently involved in these courses to help beneficiaries.



The investment made by beneficiaries, through the co-financing of selected projects, is on average more than 20% higher than expected, showing both the strong need for the solution, and the awareness of the stakes. The mobilization of these resources over the long term, through an increased cyber budget and dedicated human resources, should make it possible to sustain the actions that ANSSI has helped to initiate. It should be noted that more than 95% of the security solutions acquired as part of the cybersecurity program are European.

The rise of a network of regional CSIRTs

The creation of a cyber incident response center in each region is a relevant solution to support victims from mid-sized organizations in both the private and public sectors facing the multiplication of cyberattacks. The aim is to limit the economic and social impacts of cyberattacks by supporting their rapid resolution. These centers must become true incident response services of general interest, adapted to the needs of SMEs, micro-enterprises and public structures, allowing the monitoring of incidents and the connection of victims with the appropriate service providers to support them.

Through the stimulus plan, 12 out of 13 metropolitan regions have expressed their commitment and have been supported financially with a subsidy of €1M, and technically, through the monitoring of an incubation program for an accelerated start-up. 7 CSIRTs are already operational, and all of them should be operational by the end of 2023.

Overseas, these structures lean more towards the development of the local ecosystem, to bring out the offer of solutions and services while raising awareness of the threat to develop demand. One such cyber resource center is supported for the Atlantic coast (CRC Caribbean), another is supported for the Indian Ocean coast (CRC Reunion), and one is supported for the Pacific Ocean coast (CRC New Zealand).

These centers will allow in each territory the concentration of information on the attacks suffered by these intermediate size structures. They should become the contact points for victims to put them in touch with response providers.

Learn more:
The cybersecurity component of France Relance
Regional CSIRTs

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 marked by miniaturisation coupled with falling costs.** This trend, embodied by Moore's Law, has had a strong impact on the world economy over the last 50 years and is expected to continue at least over the next decade with the development of 3D multilayer memories and the miniaturisation of processors. However, this trend is coming to an end. Investments to continue Moore's Law and keep up with the innovation race are growing exponentially and have already reached such levels that only seven companies are holding their own globally: 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.

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, longdistance 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.).

That is why, **we are witnessing the construction of several sovereign cloud offers from the French ecosystem,** such as the «Numspot» offer carried by Docaposte and involving Dassault Systèmes, Bouygues Telecom and the Banque des Territoires. **Also noting the construction of the first French sovereign collaborative cloud platform** by the three companies Olvid, Oodrive and Tixeo. Other trusted cloud offerings have been built in France but in partnership with GAFAMs, leaving aside the «sovereign cloud» aspect: S3NS (Thales and Google), Bleu (Orange, Cap Gemini and Microsoft), as well as a joint offering between AWS and Atos.

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.

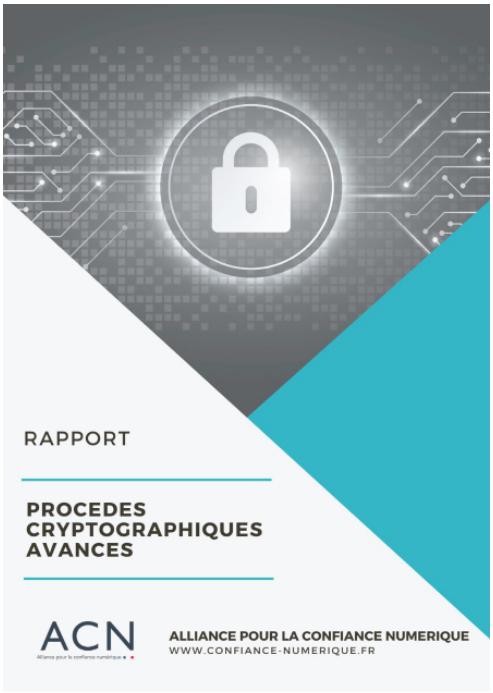
6.2 Specific Digital Trust innovations that generate new products

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 cybersecurity. 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 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
«Procédés cryptographiques avancés»
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 STMicroelectronics. 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 includes the development of machine learning algorithms (artificial neural networks, multilayer or not, supervised or not, generative adversarial networks, etc.), and the problem of edge AI, i.e. the design of chips and embedded systems dedicated to the use of machine learning algorithms (which are very greedy in terms of computing capacity and memory). Developments in artificial intelligence are not specific to the security sector, but numerous adaptations and applications are emerging in most segments:

■ **Behavioral biometrics.** The segments of identification and authentication of people, access control and intrusion detection and alarm are positively impacted by the development of behavioral biometrics solutions: facial recognition, signature recognition, identification of people by a sequence of images allowing to specify a behavior, etc.;

■ **Aggregation and analysis of data collected in the segments of local observation, wide area observation and intelligence & information;**

■ **Cybersecurity auditing.** In terms of 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). However, in terms of industrial ecosystem involved in developments around AI in general, France is far behind the United States and China, which benefit from their strong digital industrial fabric. In particular, there is a brain drain from France to the United States in this area, which threatens French positions in the future, including in the security sector.

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

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

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. Other technological developments exist, but do not have the same intensity of impact on the global digital trust industry. Developments around digital identity are an illustrative example: **captcha and challenges for software, QR codes, iris recognition, vein recognition, dynamic passwords, 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 cybersecurity 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.

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 critical decision chain in a digital environment. Atos, Orange, Equans and IBM are also positioned on global offers.

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 Alliance pour la Confiance Numérique (ACN - Alliance for Digital Trust) represents organizations (world leaders, SMEs, mid-sized enterprises and micro-enterprises) in the digital trust sector, particularly those specializing in digital identity, cybersecurity, and trusted artificial intelligence. In this field, France boasts highly efficient industrial cooperation and internationally recognized excellence thanks to world leaders, SMEs, mid-sized enterprises, and the various dynamic actors in the sector.

2,130 organizations in France generate a profit €17.7B in this rapidly growing sector (average annual growth of 7.6% since 2016).

The 106 members of the ACN, 89% of which are SMEs, micro-enterprises and mid-sized enterprises, represent 2/3 of the turnover of French digital trust companies worldwide (hardware manufacturers, software vendors, integrators, services, security assessment laboratories, research, etc.).

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

ACN is also a founding member of the European CyberSecurity Organisation (ECSO).

ACN
Alliance pour la confiance numérique

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

ACN's members

ACN's partners

ABOUT DECISION ETUDES & CONSEIL

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.

Their 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.

Version Française disponible sur :
www.confiance-numerique.fr

Partenariats Presse

JDN · groupe aef info · B SMART · DCloud dcloudnews.eu