2023

Alliance pour
la confiance numérique

confiance-numerique.fr

Observatoire de la Filière de la Confiance Numérique

ACN
Alliance pour la confiance numérique

SOMMAIRE

LE MOT DE L'ACN - ALLIANCE POUR LA CONFIANCE NUMÉRIQUE

Daniel Le Coguic
Président de l'ACN

Plus que jamais, la Confiance Numérique est au cœur des enjeux de nos sociétés. Le numérique tend à devenir le mode préférentiel pour tous nos échanges, dans notre vie quotidienne, dans nos activités économiques, dans notre relation avec l'Etat, mais aussi dans la sphère géopolitique.

A ce titre, l'espace numérique devient, chaque jour un peu plus, le terrain d'expression de l'ensemble des comportements et des besoins qui sont l'apanage habituel du monde physique, ces derniers étant accélérés, démultipliés, dématérialisés.

La confiance est la pierre angulaire des relations humaines depuis que l'Homme s'est organisé en communautés. Elle est la base de toute vie en commun et elle structure les édifices juridiques de toute société, qu'il s'agisse de régir les interactions entre individus, ou d'assurer l'ordre public ou international. Depuis sa création, le numérique s'est construit essentiellement sur une vision utilitariste : sa puissance et sa diffusion massive viennent aujourd'hui questionner nos sociétés et nos règles de fonctionnement, conçues pour réguler des interactions physiques.

Toutefois, réguler le numérique en ne s'attaquant qu'à ses effets dystopiques une fois qu'ils ont été constatés revient à traiter les symptômes plutôt que les causes, ainsi nous condamne à un retard, à une inadaptation perpétuelle des réponses apportées. Il est urgent de revenir aux fondamentaux et de poser comme principe intangible que la confiance dans le numérique est la base de son déploiement.

Les outils qui concourent à la Confiance Numérique sont nombreux. L'identité numérique est une clé d'entrée certaine : dans le monde physique comme dans le monde numérique, point de confiance si l'on ne peut être certain que l'on est face au bon interlocuteur. La cybersécurité est également un axe majeur : nous devons être sûrs que les interactions numériques se déroulent telles qu'elles ont été souhaitées, sans intrusions, sans déformations, sans possibilité de les interrompre. Enfin, la puissance de l'intelligence artificielle doit impérativement être encadrée, régulée par cette Confiance Numérique.

Le Gouvernement a parfaitement saisi cette vision, en posant la Confiance Numérique comme

ambition première du projet de loi « Sécuriser et Réguler l'Espace Numérique » et en déclinant des mesures pour protéger nos concitoyens, en particulier les enfants, nos entreprises et nos collectivités, ainsi que notre démocratie. Ces mesures, présentées par le Ministre Jean-Noël Barrot, en appellent beaucoup d'autres. L'ACN soutient la vision holistique qui a été adoptée. Les déclinaisons de cette vision sont sociétales, économiques, démocratiques, mais aussi géopolitiques. Au niveau européen aussi, l'heure est à la construction de règles visant à atteindre les mêmes objectifs de régulation et de sécurisation de l'espace numérique. Sous l'égide du commissaire Thierry Breton, de nombreuses initiatives sont en cours (directive NIS2, règlement *Cyber Resilience Act*, projets de règlements sur un portefeuille européen d'identités numériques, projet d'*AI Act*, ...).

La France a la chance de disposer de tous les outils pour renforcer sa souveraineté numérique, maîtriser son avenir numérique et contribuer de manière décisive à l'autonomie stratégique française et européenne. La filière de la Confiance Numérique se compose d'un écosystème d'entreprises solide, dynamique et agile, composé tant de grands leaders mondiaux que de start up et PME d'excellence. Chaque année depuis plus de 10 ans, l'ACN scrute, à travers son Observatoire, les évolutions de cette filière et en décrypte les principales tendances.

En 2022, la filière de la Confiance Numérique a connu sa plus forte croissance depuis 2015 (+10,1% de chiffre d'affaires). Cette croissance, supérieure de 3 points au rythme moyen de progression de ces 5 dernières années, conforte l'analyse d'un secteur porté par des tendances de fond très solides telles que la transformation numérique, le développement du télétravail, le maintien de la menace à un haut niveau, le contexte réglementaire et la prise de conscience des entreprises et institutions...

Cette dynamique ne doit toutefois pas masquer l'ampleur des défis qui nous font face : afin de pouvoir répondre aux besoins nombreux, identifiés et à venir, pour protéger notre pays, améliorer la résilience de tous, et préserver notre souveraineté numérique, la filière française de la Confiance Numérique doit parvenir à attirer et à former des talents en masse, mais doit aussi se structurer efficacement. En effet, les enjeux sont à la fois nationaux et européens, et de notre capacité à concentrer nos efforts et à agir de manière collective et coordonnée dépend l'influence que nous pourrons exercer à cette échelle. C'est précisément le rôle d'une organisation professionnelle telle que l'ACN que d'assurer la synergie et la représentation institutionnelle efficace de cette filière stratégique.

Dans le monde numérique, beaucoup reste à écrire et notre filière est convaincue de montrer une voie originale dans un monde multipolaire toujours plus conflictuel. Cette voie consiste à porter dans un même élan les valeurs fondamentales françaises et européennes et les outils de Confiance Numérique qui en assurent la pérennité et la promotion.
Un mot d'ordre pour la filière : développer et mettre à disposition des outils compatibles avec les libertés publiques et acceptables pour nos concitoyens.

Capitaliser sur nos atouts et sur l'excellence de la filière française de la Confiance Numérique vise ainsi à la fois à nous protéger, à nous rendre plus résilients, mais aussi à solidifier notre modèle de société. L'Etat doit poursuivre et amplifier son effort d'accompagnement pour que notre filière, jeune et dynamique, puisse devenir le pilier de notre souveraineté numérique. Dans un contexte géopolitique de plus en plus conflictuel, où les différents blocs ne partagent pas les mêmes valeurs, il est temps de d'œuvrer collectivement au renforcement de la voix de la France pour une Europe numérique plus pacifiée, plus libre, plus innovante et plus protégée au bénéfice du plus grand nombre. Bâtissons ensemble cette France nouvelle qui deviendra le fer de lance du projet européen.

LE MOT DU MINISTRE

Crédit : Ministère de l'Economie, des Finances et de la Souveraineté industrielle et numérique

Jean-Noël Barrot

Ministre délégué chargé de la transition numérique et des télécommunications

La transformation numérique de l'économie française ainsi que l'augmentation du nombre d'objets connectés multiplient les risques cyber alors même que le contexte géopolitique est propice à la conduite de cyberattaques pouvant déstabiliser l'économie et la société. La protection des entreprises contre le risque cyber, y compris en dehors des secteurs d'importance vitale, est plus que jamais un impératif vital sur le plan économique et de la sécurité nationale.

A cet égard, la filière de la Confiance Numérique joue un rôle précieux pour accompagner les mutations numériques de notre économie et de notre société, tout en permettant à nos concitoyens de bénéficier d'un numérique plus sûr et sécurisé. Elle bénéficie naturellement du soutien du Gouvernement, qui a fait de la protection des systèmes d'information des entreprises et des organismes publics une priorité forte et, pour ce faire, entend notamment s'appuyer sur un écosystème privé robuste, souverain et innovant.

Conscient de l'importance cruciale de garantir la résilience de notre pays face à la menace, le Président de la République a annoncé une stratégie d'accélération pour la cybersécurité en janvier 2021, qui est financée à hauteur d'1 milliard d'euros par le plan France 2030. Dans ce cadre, notre ambition est de soutenir la croissance de notre industrie française et européenne de la cybersécurité, et de faire émerger des leaders à même de renforcer notre souveraineté sur ces technologies stratégiques.

Outre un accent important mis sur la R&D et sur la formation des talents, cette stratégie, dont près de 400 millions d'euros de financements publics ont déjà été engagés, vise également à développer des solutions innovantes via une suite spécifique d'appels à projets.

Parmi les thématiques traitées, on compte par exemple le développement de briques de sécurisation des outils de communication et des suites collaboratives, ou des solutions de cybersécurité pour les grands événements. Au total, ce sont 30 projets qui ont été soutenus pour près de 85 millions d'euros par la stratégie, le prochain appel à projet devant être publié courant juin 2023.

Mais les moyens pour faire face à la menace sont divers, et l'innovation technologique seule ne suffit pas. Il faut aussi former et sensibiliser. C'est pourquoi le Gouvernement s'attache tout particulièrement à structurer son action de façon coordonnée et décentralisée, pour être efficace au plus près des besoins et des territoires.

C'est tout le sens de la création du Campus Cyber en 2021, ce lieu totem de notre écosystème qui vient renforcer les synergies entre acteurs publics et privés. C'est aussi le cas des parcours de cybersécurité que l'ANSSI a pilotés au profit de près de 1000 organismes publics et qui participent directement d'une meilleure résilience cyber de nos services publics.

Au titre de la sensibilisation des acteurs économiques, j'ai en outre annoncé, en octobre dernier, un dispositif d'accompagnement financier de 750 PME et ETI sensibles dans leur démarche de cybersécurisation, basé sur 3 grands principes : une approche de bout-en-bout prenant en compte la maturité cyber des entreprises, un recrutement ciblé par secteur, et une articulation forte avec les régions. Les travaux de construction de ce programme sont proches de leur achèvement et nous pourrons recueillir les premières candidatures des entreprises éligibles au cours de l'été 2023.

Enfin, les enjeux socio-économiques et de souveraineté relatifs à l'intelligence artificielle font l'objet d'une actualité toute particulière.

Pour que l'IA soit « de confiance », elle doit garantir l'absence de défaillances, la sécurité des utilisateurs et la fiabilité des systèmes. Pour cela, le fonctionnement des algorithmes doit être sûr, explicable et responsable, notamment pour les systèmes qui peuvent engager des vies humaines ou porter atteinte aux droits des individus. Il s'agit ici d'un prérequis indispensable pour la bonne acceptabilité de toute technologie par les citoyens.

Il est essentiel de se doter de solutions technologiques permettant à l'écosystème français de développer des produits et services en conformité avec les exigences de la future règlementation européenne (*AI Act*). En effet, au-delà de l'investissement, le développement de l'IA de confiance passera également par la mise en place d'un cadre réglementaire clair et adapté. La France, qui a activement participé aux négociations sur le règlement IA lors de sa présidence du Conseil au premier semestre 2022, a su veiller à assurer l'équilibre entre innovation et protection.

Sur le plan de l'éthique, une réflexion devra également se formaliser. C'est la raison pour laquelle j'ai récemment saisi le Comité national pilote d'éthique du numérique, que le Président de la République a pérennisé le 9 mars dernier à l'occasion des 40 ans du Comité Consultatif National d'Ethique. Les conclusions de la saisine seront livrées au Gouvernement avant l'été.

ÉLÉMENTS CLEFS

La filière de la **Confiance Numérique** est cruciale dans notre économie et dans notre société en pleine mutation numérique.

Elle regroupe la **sécurité numérique** (identité numérique, systèmes et sous-systèmes électroniques de confiance), ainsi que la **cybersécurité** (produits / logiciels et services).

L'**Alliance pour la Confiance Numérique (ACN)** a été constituée pour regrouper et soutenir les acteurs de cette filière en France et en assurer la représentation institutionnelle.

L'ACN a mis en place un **Observatoire de la Confiance Numérique** pour recueillir et mettre en commun des données sur les grandes caractéristiques et les tendances de cette filière ; c'est dans ce cadre que cette étude a été réalisée en 2022, couvrant le champ de la cybersécurité et de la sécurité numérique.

La Confiance Numérique en France en 2022 c'est :

17,7 milliards d'euros de chiffre d'affaires en France

- **17,7 milliards d'euros de chiffre d'affaires**, soit 10,1% de croissance entre 2022 et 2021 ;
- **8,4 milliards d'euros de valeur ajoutée ;**
- **86 700 personnes employées dans le secteur ;**
- Un **chiffre d'affaires** réparti à **56% pour la Cybersécurité et à 44% pour la Sécurité Numérique.**

Les entreprises françaises de la Confiance Numérique dans le monde en 2022 c'est :

16,4 milliards d'euros de chiffre d'affaires à l'international

- **28,7 milliards d'euros de chiffre d'affaires** générés dans le monde par la filière française de la Confiance Numérique (CA France, CA exporté depuis la France et CA réalisé à l'étranger par des entreprises détenues par des capitaux français) ;
- Des **leaders mondiaux** sur les segments de la sécurité numérique (Thales, Airbus, Atos, STMicroelectronics), de la gestion des identités et des accès (Thales, Idemia, IN Groupe, Docaposte), des services de cybersécurité (Thales, Atos, Orange Cyberdefense, Sopra Steria, Capgemini), et de la sécurisation des paiements (Worldline) ;
- **16,4 milliards d'euros de chiffre d'affaires à l'international**, soit 57% du CA total (CA exporté depuis la France et CA réalisé à l'étranger par des entreprises détenues par des capitaux français) ;
- **5,4 milliards d'euros de chiffre d'affaires à l'exportation depuis la France**, soit un taux d'export moyen de 31%.

La Confiance Numérique est une filière à part entière :

10.1% de croissance en France en 2022

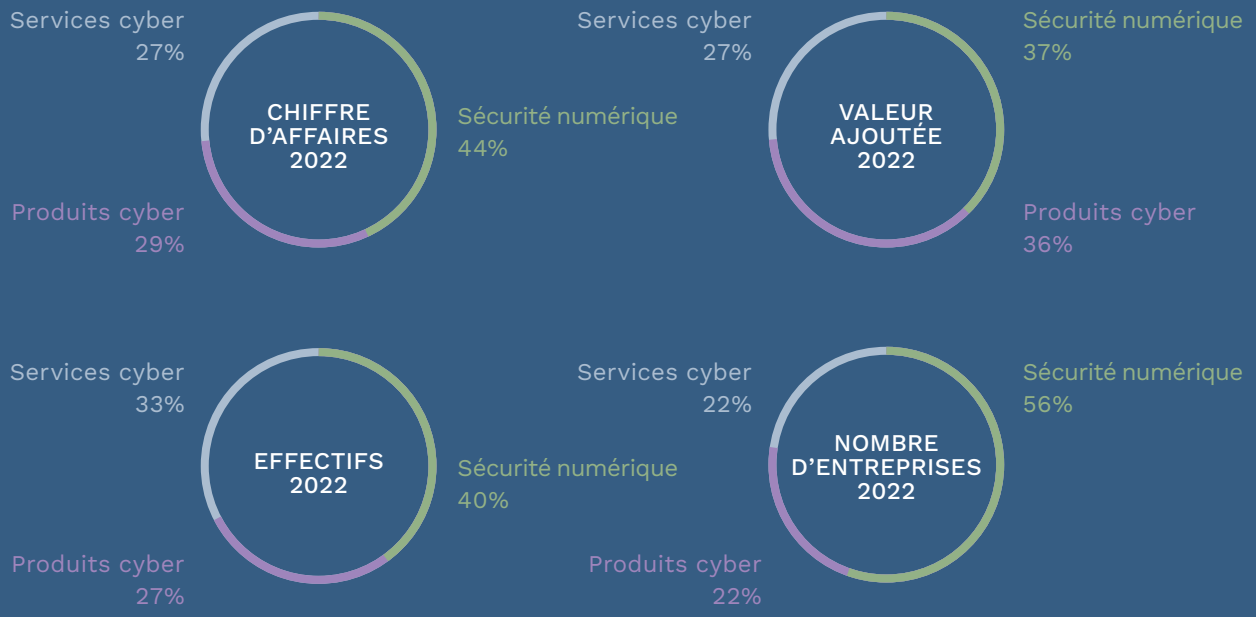
- **7,5%** de croissance moyenne annuelle en France sur la période 2017-2022, contre **1,0%** pour le PIB français (Croissance du PIB mesurée par l'INSEE en volumes chainés, FMI pour l'année 2022) ;
- La Confiance Numérique est la **filière industrielle française qui bénéficie de la croissance la plus forte**, et ce depuis 10 ans ;
- **La Confiance Numérique s'est montrée particulièrement résiliente face à la crise COVID en 2020, avec 3,6% de croissance en 2020** contre -7,8% pour le PIB français ;
- La Confiance Numérique est **la filière la plus productive**, c'est-à-dire avec le plus fort ratio Valeur Ajoutée / Chiffre d'affaires.

La Confiance Numérique est un écosystème d'entreprises de toutes tailles :

2 129 entreprises dans la filière en France

- **2 129 entreprises** dans la filière en France ;
- Dont **75 grandes entreprises ;**
- Dont **67 ETI** (Entreprises de Taille Intermédiaire) ;
- Dont **644 PME** (Petites et Moyennes Entreprises) ;
- Dont **1 343 micro-entreprises**, générant moins de 2 millions de CA en 2022.

Les principaux segments de la Confiance Numérique



Sources : DECISION études et conseils

FONDAMENTAUX 2022

Chiffre d'affaires

28,7 MDS € de CA monde

- 11 MDS € de CA hors France
- 17,7 MDS € de CA France
  - dont 5,4 MDS € de CA Export

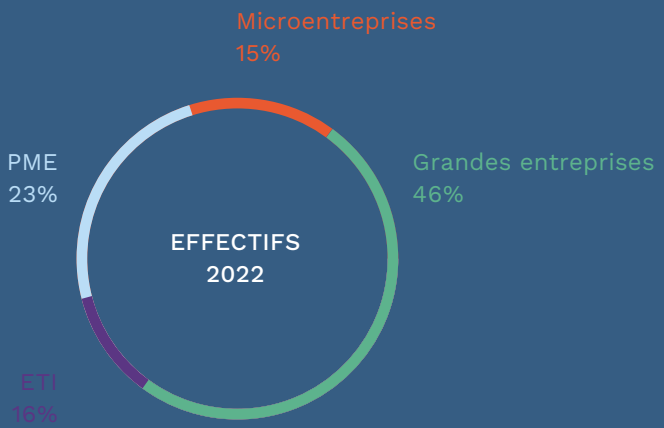
8,4 MDS € VA* France

*(valeur ajoutée)

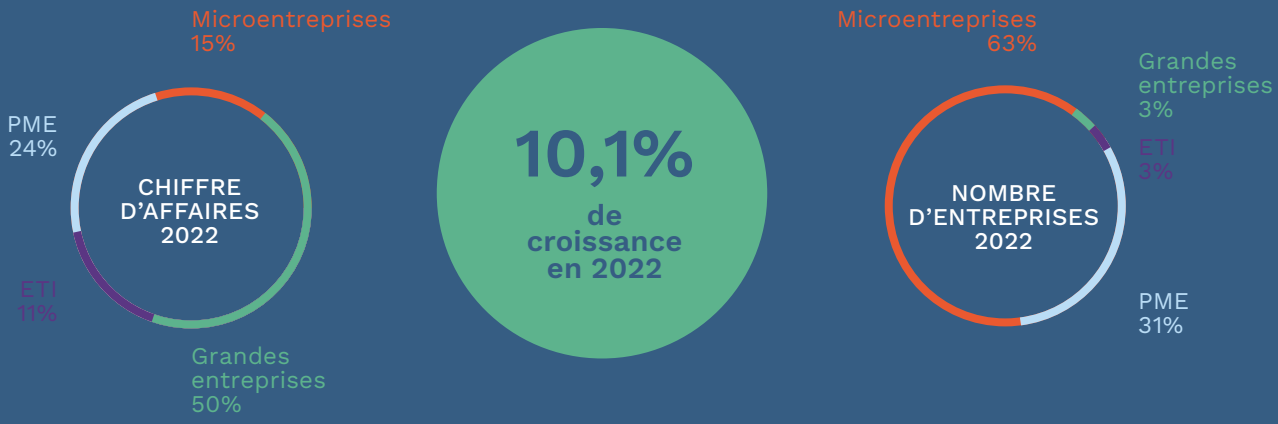
Emplois

86 700
Emplois en France en 2022

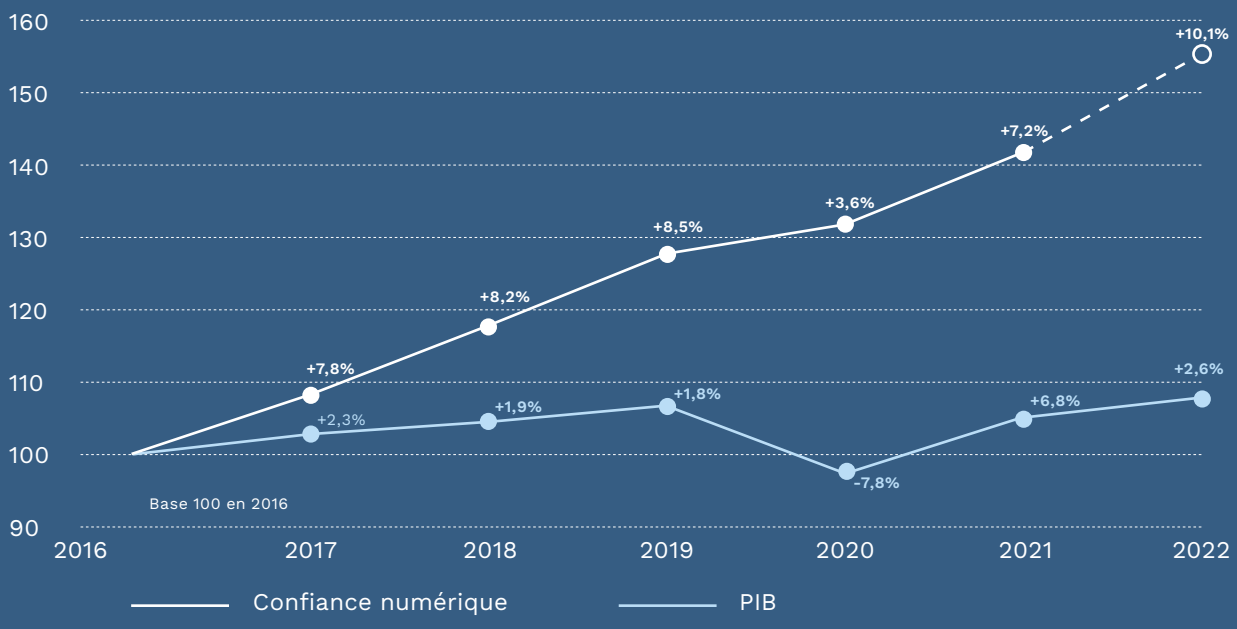
138 100
Emplois dans le monde en 2022



Croissance



Croissance France comparée 2017-2022



Croissance du PIB mesurée par l'INSEE et par le FMI pour l'année 2022

Source : DECISION Etudes & Conseils

Top 10 acteurs France

N°	Entreprises	CA Confiance Numérique 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 comprend Gemalto et Ercom.
- Atos comprend Idnomic, Ipsotek, Motiv ICT Security, Sec consult, In fidem, Paladion...
- Orange Cyberdéfense comprend Securelink, Securedata, Lexsi...
- Sopra Steria comprend CS Group, Tobania, Ordina, Sodifrance, Bluecarat, Kentor, Eva Group...
- Capgemini comprend Altran et Leidos Cyber.
- Docaposte comprend AR24, CDC Arkhineo, Open Value...
- Accenture comprend Arismore, Link by net, Openminded...
- Chapvision / Flandrin technologies comprend Deveryware, Bertin IT, Vecsys et Elektron.
- Idemia comprend Otono Networks.
- IN Groupe comprend Surys et Nexus.
- Econocom comprend Exaprobe.
- Wordline comprend Ingenico.
- GFI Informatique comprend SIS.
- Cisco comprend Sentryo.
- Securitas comprend Stanley Security.
- Sogetel comprend Eryma.

Emergence d'un écosystème de distributeurs de produits et services de cybersécurité

Top 1-10 acteurs France

Top 10-20 acteurs France

CA Confiance Numérique France compris entre 100M€ et 230M€

Top 20-50 acteurs France

CA Confiance Numérique France compris entre 40M€ et 100M€

Les drapeaux indiquent la nationalité des capitaux des acteurs présents en France.

Top 10 acteurs monde - 2022

N°	Entreprises	CA Confiance Numérique Monde
1	**THALÈS**	5 288 M€
2	**ACCENTURE**	4 146 M€
3	**IBM**	3 111 M€
4	**IDEMIA**	2348 M€
5	**AIRBUS**	1884 M€
6	**ATOS**	1470 M€
7	**ORANGE CYBERDEFENSE**	977 M€
8	**SOPRA STERIA**	518 M€
9	**IN GROUPE**	445 M€
10	**DOCAPOSTE**	380 M€

La filière de la Confiance Numérique en France bénéficie de leaders européens et mondiaux :

■ **Thales** a créé un leader mondial de la sécurité numérique avec le rachat de Gemalto en 2019.

■ **Thales, Idemia, Docaposte** et **IN Groupe** sont des leaders mondiaux de l'identité numérique, de l'identification et de l'authentification.

■ **Airbus Defence & Space** est l'un des leaders européens en sécurité numérique et mondial en observation large zone et communications sécurisées.

■ **Atos, Orange, Sopra Steria** et **Capgemini** sont les 4 leaders français parmi les entreprises de services du numérique (classement SITSI), et sont également des leaders français en matière de cybersécurité (avec T**hales** et **Airbus Defence & Space**).

■ **Docaposte** est un leader français présent sur de nombreux segments de la sécurité numérique et des produits cyber. Docaposte est à l'initiative d'une offre de cloud souverain « Numspot », annoncée à l'automne 2022. En collaboration avec Dassault Systèmes, Bouygues Télécom et la CDC, cette offre de cloud souverain permettra d'opérer des services de confiance bénéficiant de la qualification SecNumCloud.

■ L'américain **Accenture** fait son entrée dans le TOP 10, porté par une forte croissance et de nombreux rachats (Arismore...).

L'ACN EST AU COEUR DE LA FILIÈRE

Parmi les adhérents de l'ACN, on trouve :

■ **14 grandes entreprises ou ETI, parmi lesquelles les 10 leaders français de la Confiance Numérique.**
■ Mais aussi **92 PME, TPE et startups innovantes adhérents directs** et **plus de 200 PME du secteur** via les écosystèmes de ses membres partenaires (GICAT, Bretagne Développement Innovation, Pôle SCS, SPAC, etc).

Les membres de l'ACN représentent :

64%

du CA des entreprises francaises dans le monde

14,5 mds € en 2022

82%

du CA des entreprises francaises dans le monde en sécurité numérique

64%

du CA des entreprises francaises dans le monde en cybersécurité

79%

du CA réalisé à l'internationnal par les entreprises francaises

10.7 mds € en 2022

I. CONFIANCE NUMÉRIQUE : CYBERSÉCURITÉ ET SÉCURITÉ NUMÉRIQUE

Parmi les acteurs situés entre la 10ème et la 20ème position et réalisant un CA Confiance Numérique supérieur à 100M€ depuis la France en 2022, on trouve -outre Cap Gemini- des acteurs français tels que Worldline (sécurité des paiements), Safran (sécurité numérique), Naval Group (cyber embarquée dans les navires), Crosscall (communications sécurisées) et STMicroelectronics, mais aussi des acteurs étrangers: Assa Abloy (contrôle d'accès), Linxens (cartes à puces), Fortinet (produits cyber), et Econocom (services cyber).

Les entreprises situées aux environs de la cinquantième position dans la filière ont des CA France de Confiance Numérique qui avoisinent tous les 40 M€ : Somfy, Securitas (Stanley Security), Serma Safety & security, Schneider, Honeywell, Palantir, Devoteam, SAP, Oracle, Apixit, Inetum, DXC, Claranet, Neurones, Computacenter, Scalian... Enfin, si les acteurs français dominent largement le top 10 de la filière, on trouve parmi les acteurs du top 10-50 une plus forte présence d'entreprises étrangères implantées en France, en particulier américaines.

1.1 Cybersécurité et Sécurité Numérique : deux domaines complémentaires

La Confiance Numérique est la garante du progrès numérique. Au fil des ans, elle est devenue un enjeu sociétal et industriel aussi important que le développement des technologies numériques elles-mêmes, car il en va de la confiance qu'on peut avoir dans ces technologies qui désormais sont au cœur de toutes nos activités. La Confiance Numérique traduit, pour tout individu ou organisation, l'assurance que les systèmes numériques qui l'affectent sont sécurisés et qu'ils vont permettre d'améliorer sa sécurité physique, financière, d'image, et en même temps protéger sa vie privée et ses données (y compris personnelles).

L'Observatoire de la Confiance Numérique couvre deux industries :

1. **La Cybersécurité** proprement dite, qui correspond à la sécurisation «interne» des systèmes numériques. La cybersécurité regroupe deux types d'activités souvent associées dans la pratique, les services (conseil, conception, mise en place, exploitation, formation), et les logiciels et solutions, destinés aux marchés professionnels (Etat et secteur public, installations critiques, entreprises, PME) et grand public (ordinateurs, smartphones, maison, véhicules et objets connectés, etc).

2. **La Sécurité Numérique**, c'est-à-dire les produits et solutions électroniques de mise en œuvre de systèmes numériques pour instaurer la confiance dans le monde extérieur. Ces systèmes mettent en œuvre des moyens numériques sécurisés pour instaurer la confiance dans l'environnement citoyen, en particulier par la gestion des identités, la gestion des accès, la biométrie, les transactions, les objets et les véhicules connectés, les processus industriels et la logistique, les transports, les réseaux, les villes intelligentes, etc. Les produits de sécurité numérique sont des produits matériels (cartes à puce, documents, lecteurs, etc.) ou des équipements (gestion des accès, biométrie, détection, localisation, etc.).

1.2 Le Périmètre de la Confiance Numérique - Segmentation

Le diagramme ci-dessous présente les différents segments de la Confiance Numérique, répartis en trois domaines :

La sécurité numérique

Controle d'accès

Systèmes complets

Identification & Authentification des personnes

Biométrie / Cartes à puces / Badges, cartes ID, etc. / Reconnaissance de véhicules / Lutte contre la contrefaçon

Observation large zone

Systèmes optroniques / Radars / wImagerie par satellite

Traçage et localisation

Etiquetage et traçage (RFID, code barres, Wi-Fi...) / Systèmes AIS, LRIT, etc. / Scellements électroniques avec suivi et positionnement (GPS, RFID)

Communications sécurisées

Systèmes optroniques / Radars Imagerie par satellite

Communications sécurisées

Communications sécurisées, alerte et information publique

Commande contrôle Aide à la décision

Renseignement Collecte d'information

La cybersécurité

Produits / Logiciels

Gouvernance cyber

Systèmes de gestion / SIEM

Gestion des identités et des accès

Sécurité des données

Chiffrement, cryptographie, signature numérique / Infrastructures à clés publiques / Gestion des droits numériques / Filtrage des contenus et anti-spam Archivage sécurisé

Sécurité des applications

Développement logiciels / OS sécurisés / Plateformes de bug bounty

Sécurité des infrastructures numériques

Firewalls / antivirus / anti-dos / détection d'intrusion / Cyberthreat / Sécurité des communications: téléphonie. visioconférence et messagerie Plateformes sécurisées de télétravail / Cloud de confiance / Blockchain

Sécurité des produits & équipements

HSM / Secure elements

Services

Audit, planning et conseil cyber

Test de vulnerabilités / Evaluation des risques, PASSI / Analyse et gestion des risques et menaces / Conseil en stratégie, planification et gestion de la sécurité / Certification en sécurité, évaluation de la conformité, CESTI / Forensics, investigation et analyse

Mise en oeuvre cyber

Gestion de projet, modélisation ingénierie et architecture / Intégration implémentation et test / Support projet

Sécurisations de l'infogérance exploitation Support d'exploitation

Supports d'exploitation Services de sécurité infogérés, gestion des opération du service de cybersécurité / Sécurisation de l'infogérance Gestion de la continuité et récupération / Tiers de confiance et services de gestion du contenu et de la réputation

Formation cyber

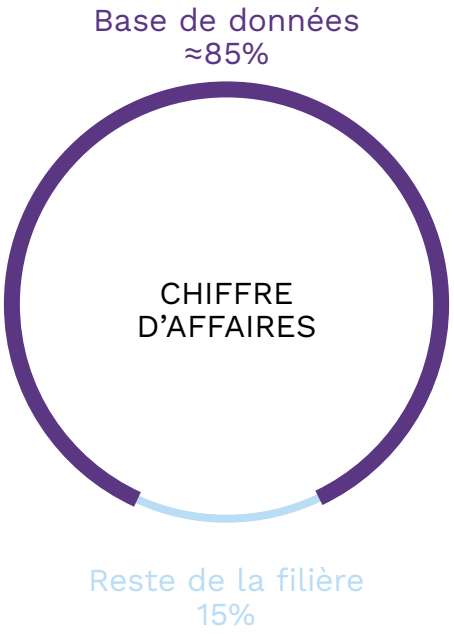
1.3 Méthodologie

L'objectif de l'Observatoire de la filière de la Confiance Numérique est à la fois de définir le périmètre de la filière et d'en évaluer le poids économique et les caractéristiques. Le cabinet d'études DECISION Etudes & Conseil conduit cet Observatoire depuis 2017.

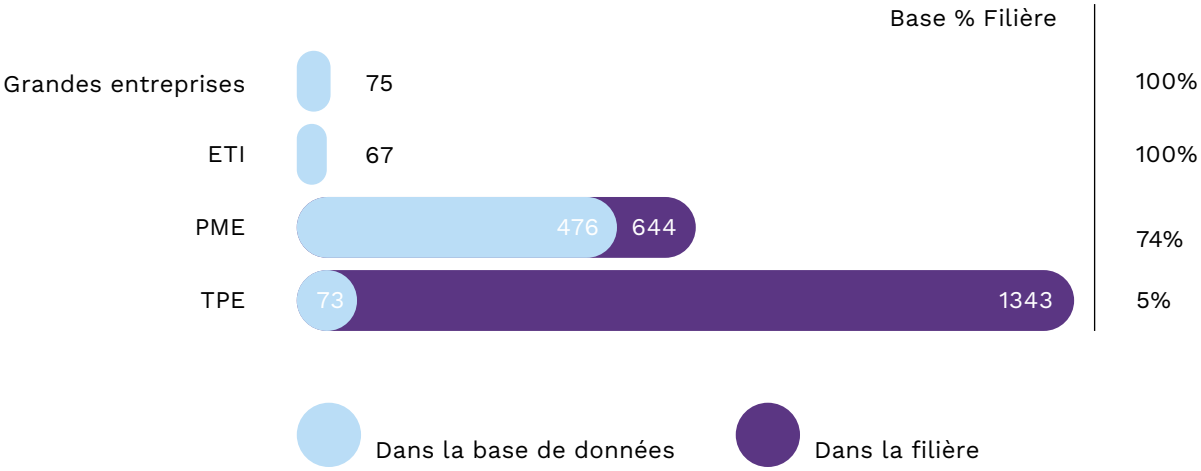
Les données présentées dans ce rapport sont issues d'une base de données de DECISION recensant 691 entreprises parmi les 2 129 que compte la filière de la Confiance Numérique. Cette base de données prend en compte :

- La totalité des grandes entreprises de la filière (75/75) ;
- La totalité des entreprises de tailles intermédiaires (ETI) de la filière (67/67) ;
- La majorité des petites et moyennes entreprises (PME) de la filière (476/644) ;
- Les très petites entreprises (TPE) et startups les plus remarquables et innovantes (73/1343).

Ainsi, bien que seul 32% des entreprises de la filière soient prises en compte dans la base de données, celle-ci est représentative de 85% du chiffre d'affaires total de la filière de Confiance Numérique France.



Nombre d'entreprises



Collecte d'information pour la base de données

Pour chaque entreprise de la base de données sont collectées chaque année les données suivantes pour la France :

■ Les données administratives : SIREN, SIRET, adresse, code NAF, nom de l'actionnaire principal du groupe, date de création, nom et fonction du dirigeant, contacts (mail, numéro de téléphone), etc.
■ Les données économiques sur la période 2015-2022 : Chiffre d'affaires, effectifs, chiffre d'affaires à l'exportation, valeur ajoutée, résultat net.

Analyse des acteurs et segmentation

DECISION effectue ensuite une analyse spécifique à chaque entreprise afin d'estimer la part de l'activité dédiée à la Confiance Numérique et la répartition du chiffre d'affaires selon les 16 segments de l'ACN (la segmentation ACN est désormais pleinement intégrée dans la segmentation plus large du Comité Stratégique de la Filière des Industries de Sécurité). Cette analyse des entreprises est réalisée grâce à l'expertise de DECISION sur le secteur de la sécurité depuis 10 ans, et notamment grâce aux entretiens directs conduits avec les acteurs clefs de la filière. Enfin, un questionnaire en ligne est envoyé chaque année aux membres de la filière et permet d'affiner les analyses.

A partir des informations de la base de données, une méthode d'extrapolation a été mise en place afin de construire des chiffres pour l'ensemble de la filière en France.

Calcul de la croissance

La **croissance** en France est estimée chaque année sur chacun des segments à travers un arbitrage entre trois composantes :

■ **Base de données** : Une analyse en sous-échantillon est effectuée afin de mesurer la croissance totale en France des acteurs représentatifs de chaque segment, c'est-à-dire des entreprises réalisant plus de 10% de leurs chiffres d'affaires grâce à leurs activités sur le segment concerné.

■ **Documents issus des entreprises** : L'analyse des rapports annuels, des documents financiers et des communications des entreprises de la filière.

■ **Questionnaire en ligne** : Le questionnaire en ligne renseigné chaque année par les membres de la filière fournit notamment des données sur la croissance de l'année passée. Pour l'édition 2023, les membres ayant répondu au questionnaire représentent 5% du CA de la filière en France.

Enfin, une analyse spécifique de l'évolution de l'activité mondiale (globale et sécurité), des principaux acteurs de la Confiance Numérique est effectuée chaque année pour estimer le chiffre d'affaires réalisé par la filière à l'étranger ainsi que son évolution.

COMPARAISONS PAR RAPPORT AUX PRÉCÉDENTS OBSERVATOIRE

Chaque année, en plus de l'estimation de la croissance, DECISION affine la segmentation des différents acteurs de la filière, notamment grâce aux informations issues du questionnaire en ligne.

En conséquence, **les chiffres en valeur absolue de chaque édition de l'Observatoire ne sont pas directement comparables entre eux**. Les chiffres de cet Observatoire sont présentés pour l'année 2022 et en fonction de la nouvelle segmentation des acteurs. Les chiffres 2021 actualisés sont présentés chapitre 3.1 de ce rapport.

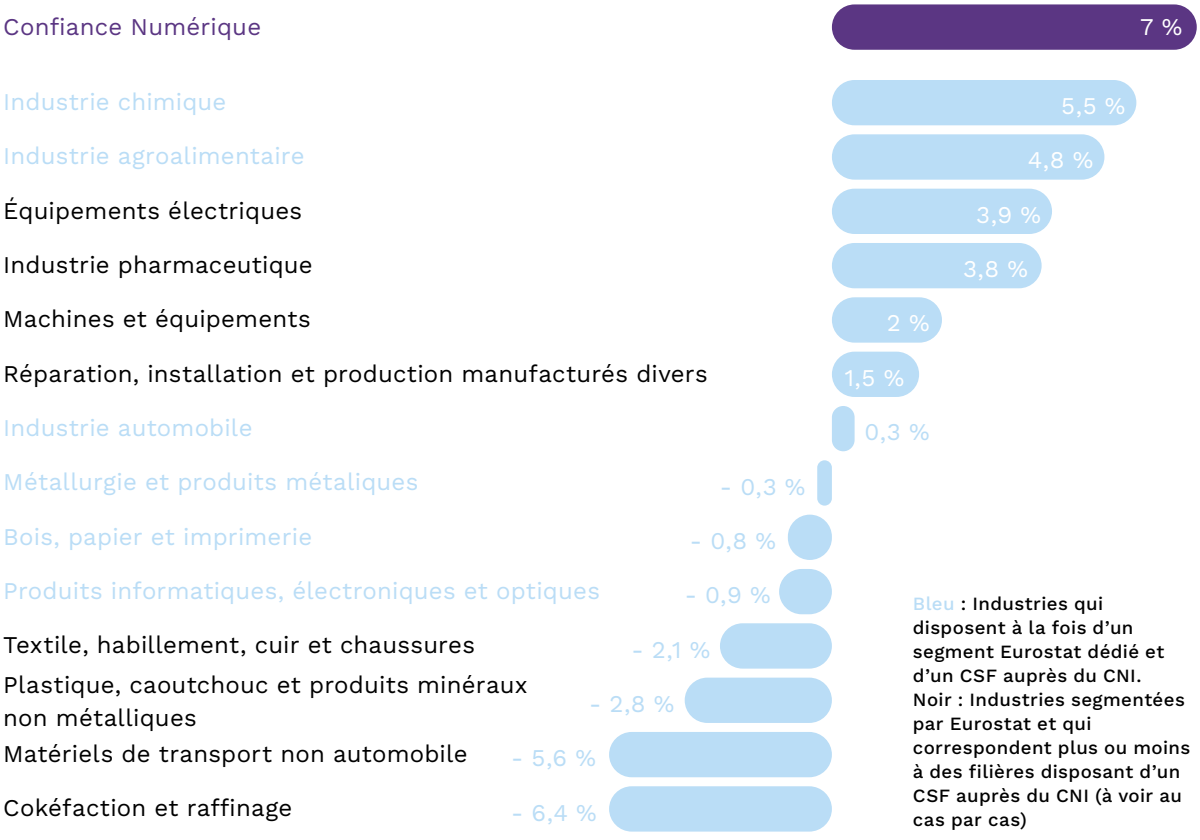
II. CONFIANCE NUMÉRIQUE : UNE FILIÈRE IMPORTANTE ET DYNAMIQUE

2.1 La Confiance Numérique est l'industrie française qui bénéficie de la croissance la plus forte sur la période 2016-2020

Sur la période 2016-2020, la Confiance Numérique est l'une des filières industrielles françaises qui bénéficie du plus fort taux de croissance, avec 7%/an en moyenne. Bien que mesurées selon une méthode qui n'est pas directement comparable, les seules autres filières industrielles françaises qui bénéficient d'une croissance similaire sont l'industrie chimique et l'industrie des équipements électriques. Les autres filières sont largement distancées, notamment l'industrie automobile qui a particulièrement souffert depuis la crise du COVID en 2020, ou encore la métallurgie.

La Confiance Numérique est l'une des quatre filières (sur un total de quinze) à ne pas avoir souffert d'une récession en 2020. Avec une croissance de 4,5% cette année là, il s'agit de la filière qui a le mieux résisté à la crise du COVID et ses conséquences. Cette résilience traduit des besoins pérennes en biens et services de Confiance Numérique. Si bien qu'à horizon 2030, la Confiance Numérique pourrait devenir la 11ème filière industrielle française sur 15 en valeur ajoutée en dépassant à la fois la filière de l'équipement électrique et la filière bois, papier et imprimerie.

Croissance annuelle moyenne des filières Françaises sur la période 2016-2020



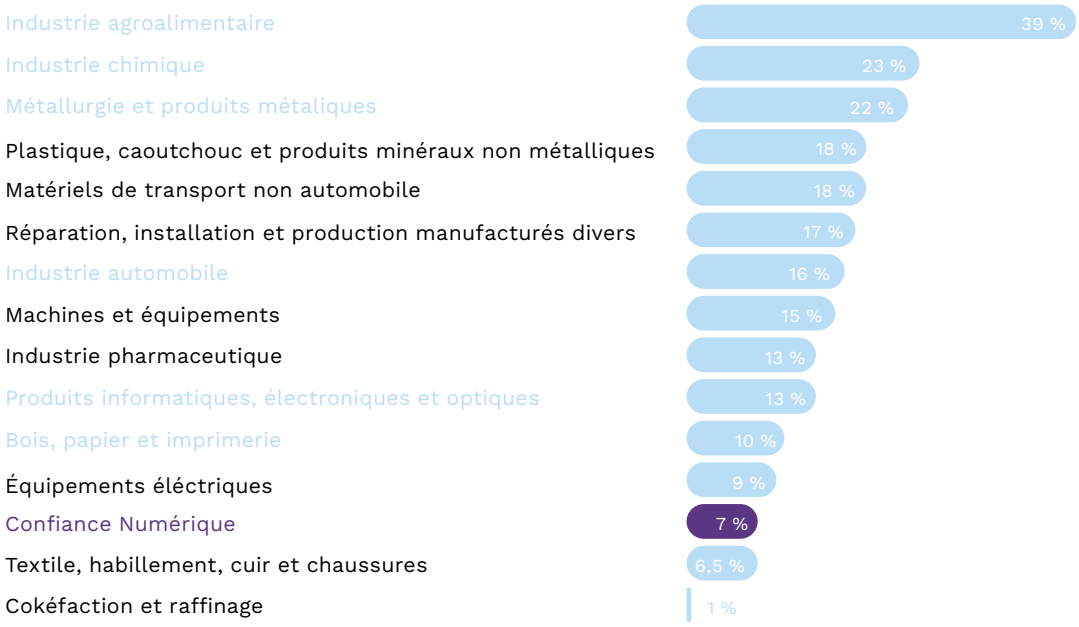
Source : Decision, Observatoire de la Confiance Numérique. DECISION, basé sur des données Eurostat jusqu'en 2020, puis sur l'évolution de l'indice de production industrielle (IPI) de l'INSEE sur la période 2019-2021.

2.2 La Confiance Numérique est une filière industrielle française à part entière

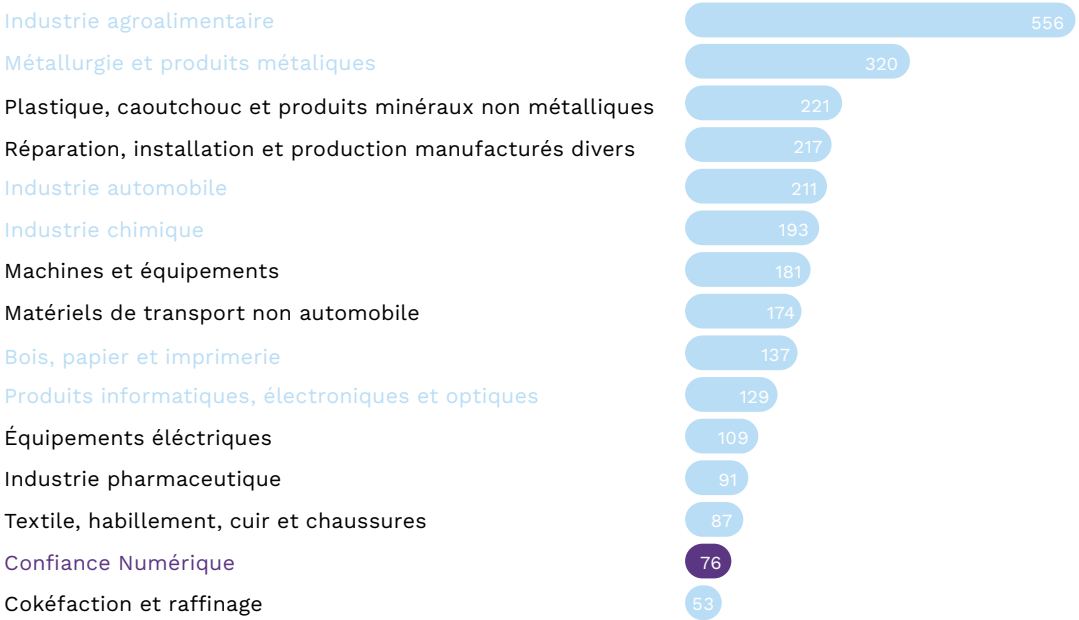
La Confiance Numérique est une filière industrielle à part entière. En termes de valeur ajoutée, elle avoisine la filière du textile et de l'habillement et se rapproche de la filière des équipements électriques ou encore du bois, papier et imprimerie.

En termes d'emploi, elle dépasse largement la filière de cokéfaction et se rapproche de la filière du textile et de l'habillement.

Valeurs ajoutées des filières françaises en 2020 (MDS €)



Emplois des filières françaises 2020 (en millier)



Bleu : Industries qui disposent à la fois d'un segment Eurostat dédié et d'un CSF auprès du CNI.
Noir : Industries segmentées par Eurostat et qui correspondent plus ou moins à des filières disposant d'un CSF auprès du CNI (à voir au cas par cas)

Source : Decision, Eurostat, OCDE

2.3 La Confiance Numérique est la filière industrielle dont l'activité est la plus créatrice de richesse en France

La Confiance Numérique est la filière la plus productive avec un taux de valeur ajoutée de 47% (Valeur Ajoutée / Chiffre d'affaires). En d'autres termes, la Confiance Numérique est la filière industrielle dont le degré de création de richesse, c'est-à-dire de transformation des produits au cours de l'activité est le plus élevé. Ainsi, l'augmentation du chiffre d'affaires de cette filière se traduit en moyenne par un plus fort taux d'activité transformatrice sur le sol français en comparaison des autres filières industrielles françaises.

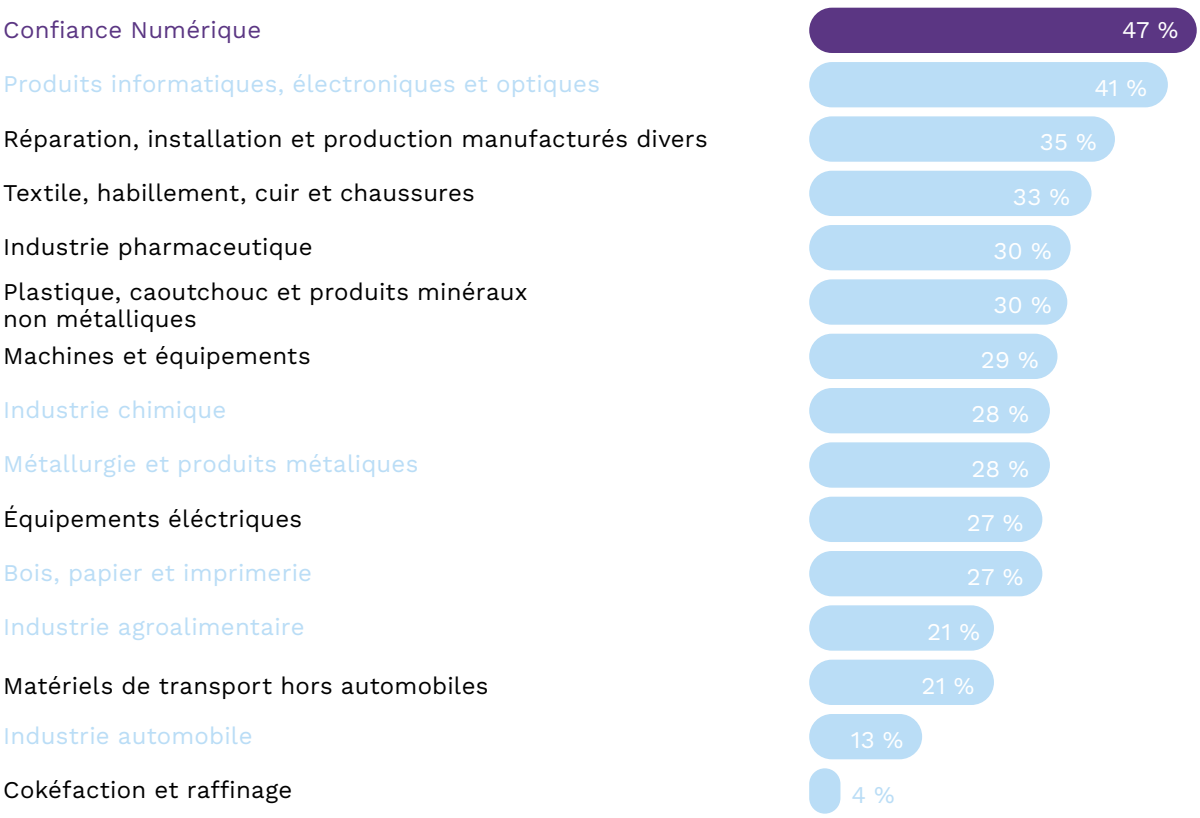
Ce phénomène s'explique principalement par trois facteurs :

1. **Le pourcentage de l'activité dédiée aux services est relativement élevé dans la filière française de Confiance Numérique** (27% en 2022), à travers les services de cybersécurité (conseil, audit, formation, etc.). Les activités de services ont par définition un taux de valeur ajoutée très fort car elles utilisent très peu de consommations intermédiaires et correspondent presque exclusivement à de la transformation des produits au cours de l'activité. Cependant, ce phénomène ne justifie pas à lui seul que l'industrie de sécurité française soit la première en matière de taux de valeur ajoutée car la plupart des filières industrielles françaises comprennent également une partie conséquente de services.

2. Les produits électroniques dédiés à la Confiance Numérique (sécurité numérique) représentent 44% du chiffre d'affaires total de la filière de la Confiance Numérique. Or, alors même qu'en ce qui concerne l'industrie électronique française dans son ensemble, une grande partie des étapes de production en amont de la chaine de valeur est réalisée en Asie, **ce phénomène ne s'applique que peu au segment de la Confiance Numérique qui maintient autant que faire se peut toutes les étapes de la production en France en raison de sa proximité avec les secteurs régaliens**. D'autres filières françaises se concentrent plus fortement sur des activités d'intégration en amont de la chaîne de valeur et sur des activités d'ingénierie pure (design, développement, etc.). Etant donné qu'une grande partie de la chaîne de valeur de l'industrie de sécurité numérique est réalisée depuis la France, le taux de valeur ajoutée augmente.

3. Enfin, les produits de cybersécurité correspondent à 29% du CA total de la filière de sécurité et impliquent **une très grande partie de travail humain hautement qualifié** (développement de logiciels, etc.), associé à un taux de valeur ajoutée très élevé (à des niveaux avoisinants ceux des services de cybersécurité).

Taux de valeur ajoutée (VA/CA des filières francaise en 2020)



Bleu : Industries qui disposent à la fois d'un segment Eurostat dédié et d'un CSF auprès du CNI.
Noir : Industries segmentées par Eurostat et qui correspondent plus ou moins à des filières disposant d'un CSF auprès du CNI (à voir au cas par cas)

Source : Decision, Observatoire de la Confiance Numérique. DECISION, basé sur des données Eurostat jusqu'en 2020, puis sur l'évolution de l'indice de production industrielle (IPI) de l'INSEE sur la période 2019-2021.

2.4 Les acteurs français sont au meilleur niveau en matière de compétences et de R&D

Grâce notamment à l'excellence française en matière de recherche et développement, **la grande majorité des entreprises françaises de la Confiance Numérique est positionnée sur les segments haut-de-gamme de leurs marchés en proposant des solutions à la pointe de ce que la technologie rend aujourd'hui possible**. La France excelle en particulier dans les domaines suivants :

Intelligence Artificielle & *Machine learning* :
La France excelle dans le *deep learning*. Les GAFAM ont installé depuis plusieurs années des centres de recherche dédiés à cette thématique et débauchent de nombreux talents français. Du côté de la R&D publique, l'INRIA dispose notamment d'équipes dédiées aux stratégies de défense et d'attaque via le *deep learning*.

Cryptographie :
La France fait historiquement partie des leaders mondiaux et maintient sa position.

Technologies post-quantique (dont cryptographie) :
La France se maintient dans le top trois mondial. D'ici quelques années, les ordinateurs quantiques devraient atteindre des stades opérationnels. La cryptographie post-quantique est donc l'un des sujets de recherche les plus critiques pour la France.

La France est également en bonne position en *blockchain* et en **sécurisation des objets connectés**. La recherche publique souffre cependant du peu d'effectifs dédiés au *Big data*. La France dispose notamment de près de 1 000 chercheurs académiques affectés à temps plein à des thématiques de cybersécurité.

2.5 La croissance de la Confiance Numérique s'inscrit dans une dynamique mondiale

Au niveau mondial, la croissance de la Confiance Numérique est portée par quatre facteurs, dont les trois premiers ne sont pas propres à la France :

1. **La miniaturisation couplée à la baisse des coûts des composants électroniques**. Ce phénomène rend possible l'intégration à grande échelle d'équipements électroniques de sécurité et participe donc d'une forte croissance en volume des équipements électroniques de sécurité.

2. **La transformation numérique**. Accélérée par la crise du COVID en 2020, les entreprises et administrations du monde entier numérisent leurs processus, déploient des *clouds* et interconnectent les réseaux de données.

3. **La croissance des pays émergents**, au premier rang desquels se trouve la **Chine**.

4. Enfin, **de nombreuses innovations technologiques** propres à la filière de la Confiance Numérique et sur lesquelles la France est souvent très bien positionnée aussi bien en termes d'acteurs industriels que de savoir-faire scientifique : biométrie comportementale, innovations associées aux éléments sécurisés, développements cryptographiques, analyse en temps réel des données d'observations large zone, *blockchain*, etc.

La France bénéficie historiquement d'une filière de défense et de sécurité puissante et fortement exportatrice au regard de la moyenne internationale et a su mettre à profit son excellence en matière de recherche et développement pour tirer profit de ces quatre tendances mondiales et ainsi construire une solide filière de Confiance Numérique. La croissance est cependant encore plus forte dans les industries de Confiance Numérique américaine et surtout chinoise.

2.6 Une concurrence croissante de la part des acteurs étrangers

Les acteurs de nationalité française génèrent 75% du chiffre d'affaires de la Confiance Numérique en France, soit 13,3 milliards d'euros en 2022. Autrement dit, **les acteurs étrangers de la filière réalisent 25% du chiffre d'affaires de la filière en France**, soit environ 4,4 milliards d'euros en 2022. Ce chiffre correspond uniquement au chiffre d'affaires généré par les filiales d'acteurs étrangers en France et n'inclut pas les exportations des acteurs étrangers vers la France (qui n'a pas pu être mesuré dans cet observatoire).

Si la part de la richesse produite en France par des acteurs français est encore assez élevée, elle baisse régulièrement depuis 2013 et cette tendance devrait se poursuivre. On assiste en particulier depuis plusieurs années au développement d'acteurs américains en France, notamment à travers l'installation de nouveaux sièges sociaux : 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... Les acteurs chinois se développent également, avec depuis peu des offres de haut niveau capables de concurrencer sur le plan technique les offres françaises.

De même que pour la production en France, le poids des acteurs étrangers sur le marché français est important : il avoisinerait les 40%. Autrement dit, le marché national reste largement influencé par des solutions étrangères et non européennes, alors que **la filière française dispose d'offres dans tous les segments et compte dans ses rangs des fleurons technologiques et de nombreux acteurs déjà de taille à couvrir à minima l'ensemble du marché national.**

Des rachats significatifs d'entreprises françaises par des acteurs étrangers ont eu lieu dans la plupart des segments de la Confiance Numérique sur la période 2013-2021. Parmi ces rachats figurent celui d'Arismore par Accenture (Etats-Unis), de DenyAll par Rohde & Schwarz Cybersecurity (Allemagne), ou encore d'Oberthur Technologies (racheté par le fond américain Advent en 2011) puis Safran Morpho (racheté par Advent en 2018). **Depuis 2021, le nombre et la taille de ces rachats tendent cependant à baisser** si bien qu'en 2022, le seul rachat d'entreprise française par une entreprise étrangère identifiée est celui d'Akka Technologies par le suisse Adecco.

Enfin et surtout, de nombreux acteurs de la filière de la Confiance Numérique relèvent une absence dommageable de culture d'achat de produits français, aussi bien de la part des entreprises que des administrations. Cette absence de culture d'achats de produits français a naturellement conduit les entreprises et les administrations françaises à se tourner vers des offres étrangères. En effet, dans un contexte général de stagnation de la croissance (1%/an de croissance du PIB français sur la période 2017-2022), et d'austérité budgétaire du côté des services publics, le premier critère d'achat s'avère souvent être le prix. Or, les acteurs américains et chinois sont souvent plus compétitifs que les français sur le seul critère du prix (notamment en raison d'économies d'échelles plus importantes et d'une sous-traitance plus forte dans des pays à faibles coûts salariaux). **En plus de pénaliser les acteurs français de la filière, l'achat de solutions étrangères non maîtrisées est susceptible de menacer la souveraineté de la France lorsque les acheteurs sont des organismes publics, des OIV (Opérateurs d'Importance Vitale), et/ou des OSE (Opérateurs de Services Essentiels)**. Malgré la récente prise de conscience des enjeux de souveraineté et d'autonomie stratégique, le manque de culture d'achat de produits français se fait particulièrement ressentir au niveau du secteur public et des grandes entreprises françaises.

Le triptyque standardisation, certification et prescription, notamment porté par l'ANSSI, permet de garantir l'utilisation de solutions fiables et sécurisées tout en déplaçant la compétition non plus uniquement sur le terrain du prix mais également sur celui de l'excellence technique, favorisant ainsi naturellement les acteurs français.

2.7 Conclusion - Une filière à très fort potentiel si les bons choix stratégiques sont réalisés

La Confiance Numérique est une filière stratégique car :

- **Le potentiel de croissance** est durablement supérieur à celui de toutes les autres industries françaises ;
- La Confiance Numérique est déjà de **taille significative** ;
- Les acteurs français sont à la pointe en matière de **compétences et de R&D** ;
- Ce secteur est essentiel à la **souveraineté numérique nationale** et à **l'autonomie stratégique européenne ;**
- Le potentiel de croissance risque d'être sous-exploité en raison de la **forte concurrence internationale**, en particulier en provenance de la Chine et des États-Unis.

Les conditions sont réunies pour que l'effet de levier en cas de mise en place d'une politique industrielle volontariste génère un maximum de retour sur investissement, aussi bien en termes d'emploi que de valeur ajoutée sur le sol français et à l'international.

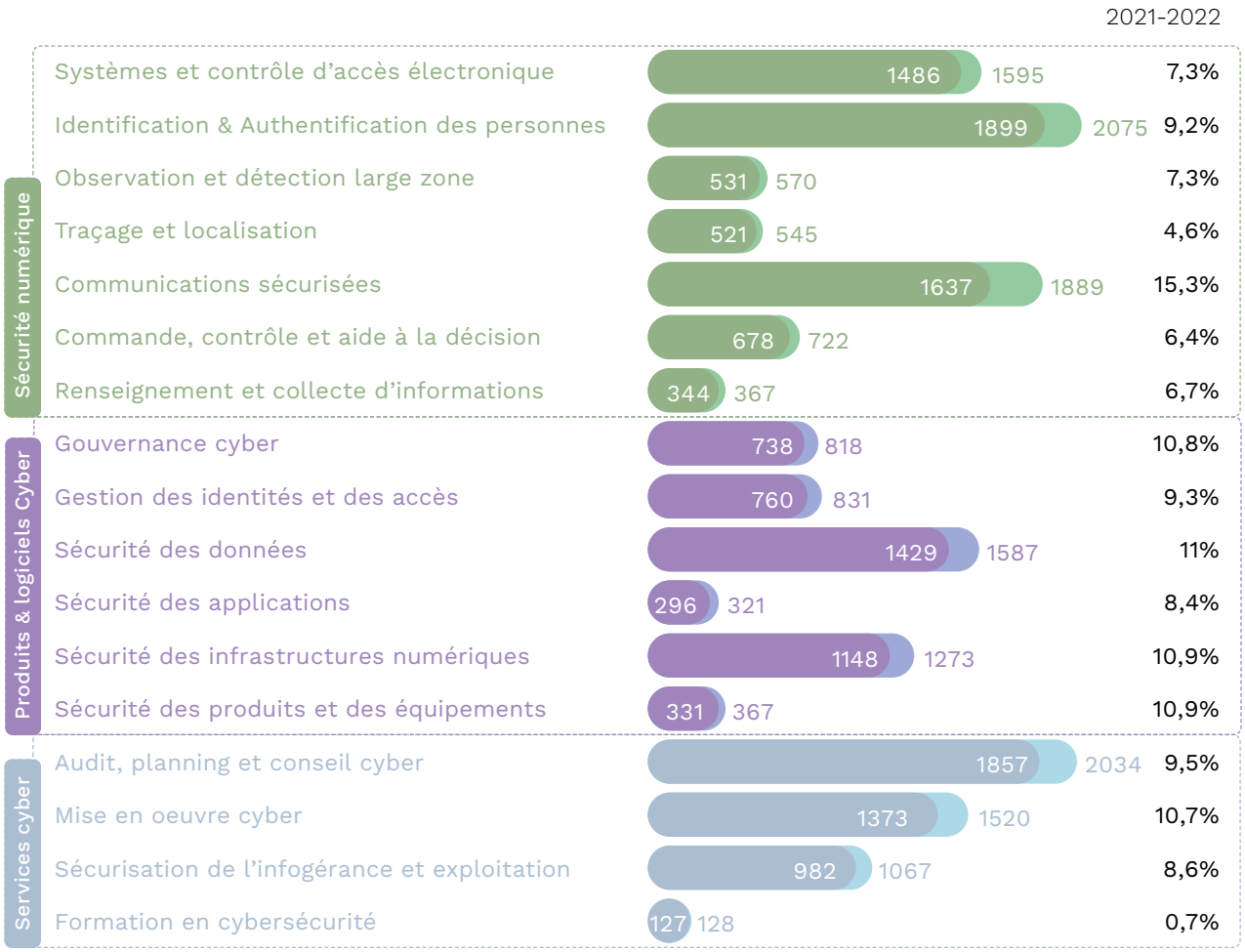
III

LES CHIFFRES CLÉS DE LA FILIÈRE

III. LES CHIFFRES CLÉS DE LA FILIÈRE

3.1 Taille et croissance

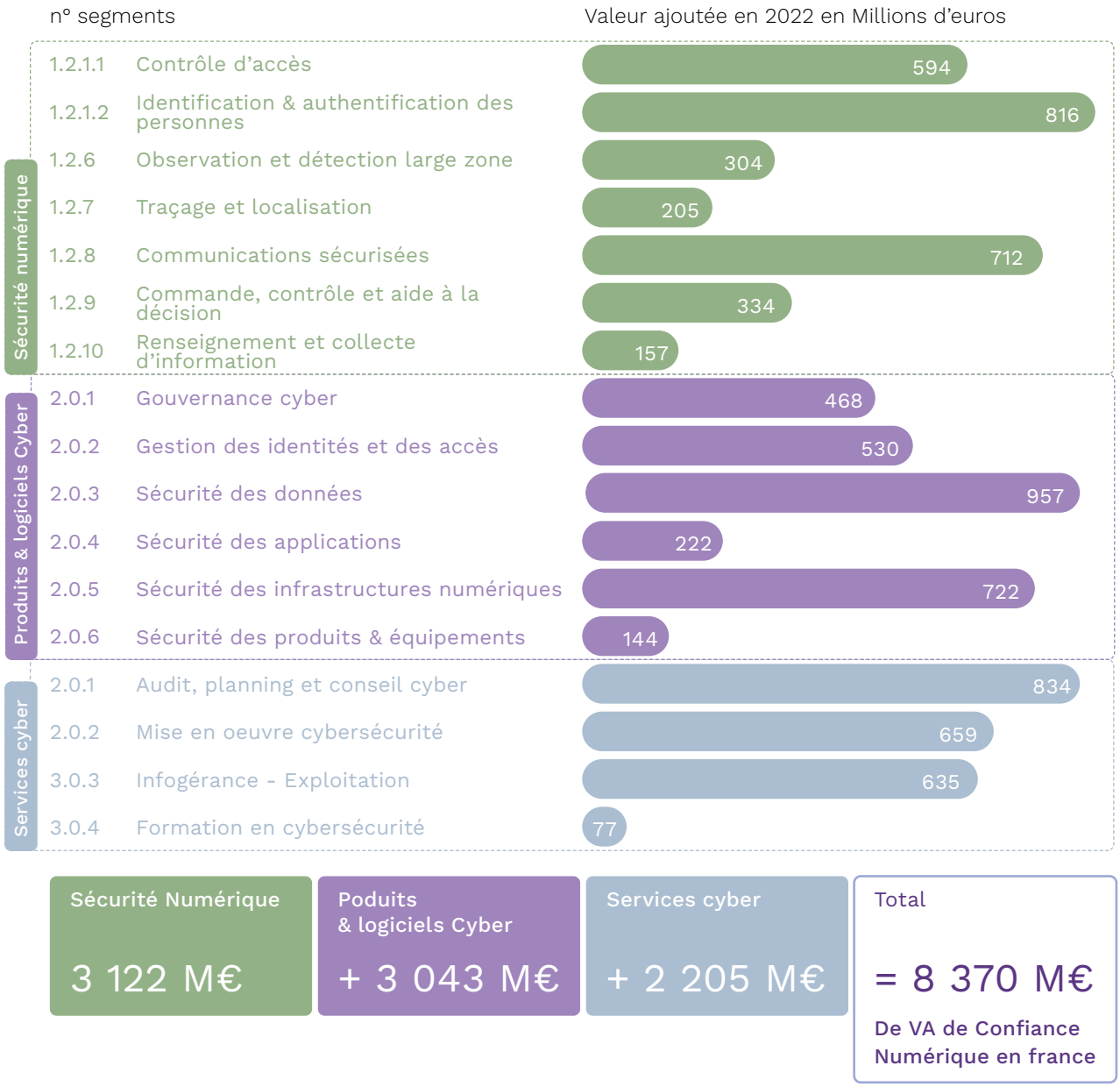
CA de la Confiance Numérique en France 17,7 Mds € en 2022



Sécurité Numérique	Poduits & logiciels Cyber	Services cyber	Total
+ 9,4%	+ 10,5%	+ 10,7%	+ 10,1%
7 762 Mds €	5 197 Mds €	4 750 Mds €	17 709 Mds €

3.2 Valeur ajoutée

Valeur ajoutée en France par segment

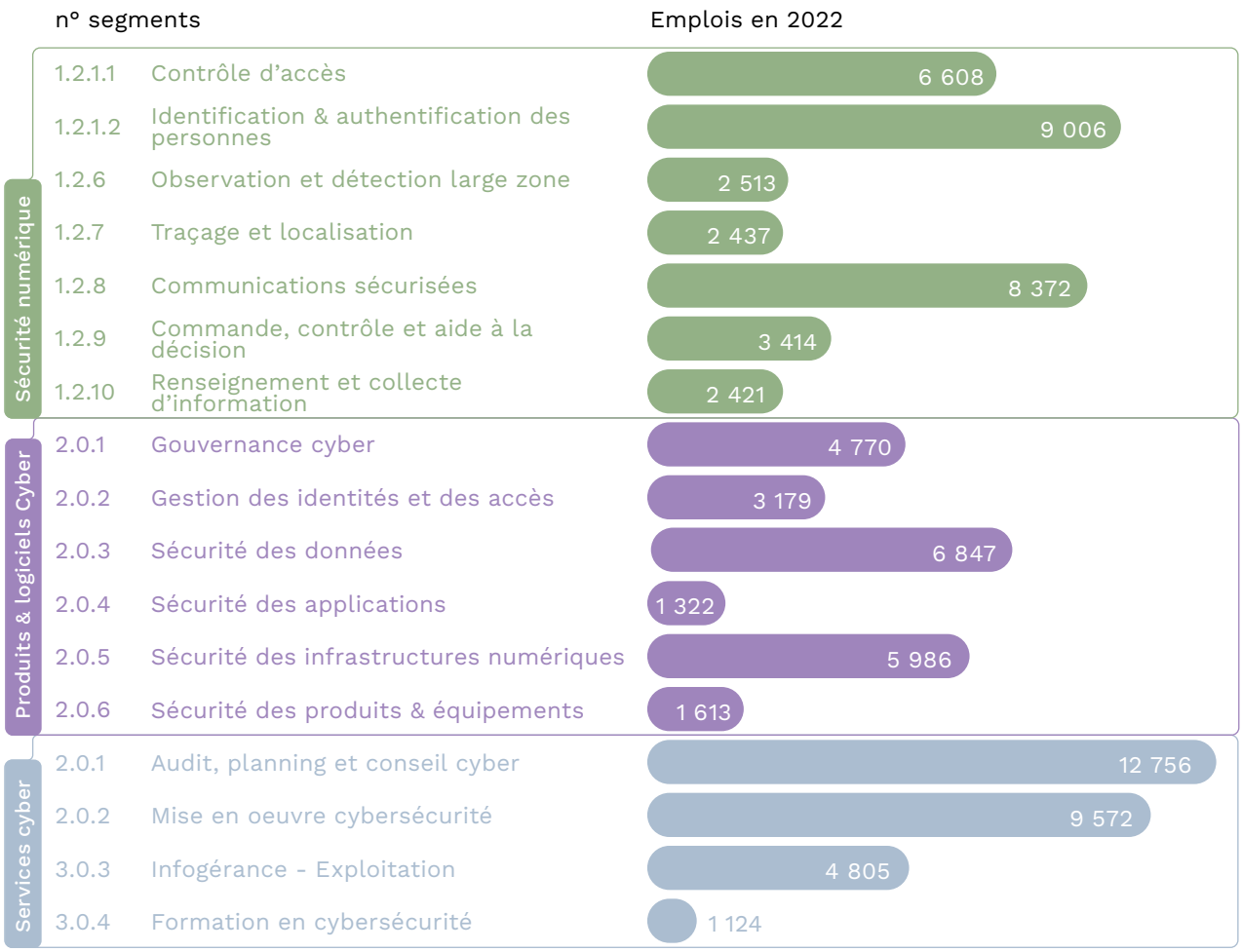


Sécurité Numérique	Poduits & logiciels Cyber	Services cyber	Total
3 122 M€	+ 3 043 M€	+ 2 205 M€	= 8 370 M€ De VA de Confiance Numérique en france

Source : Decision Etudes & conseils

3.3 Emplois

Emplois en France en 2022 par segment

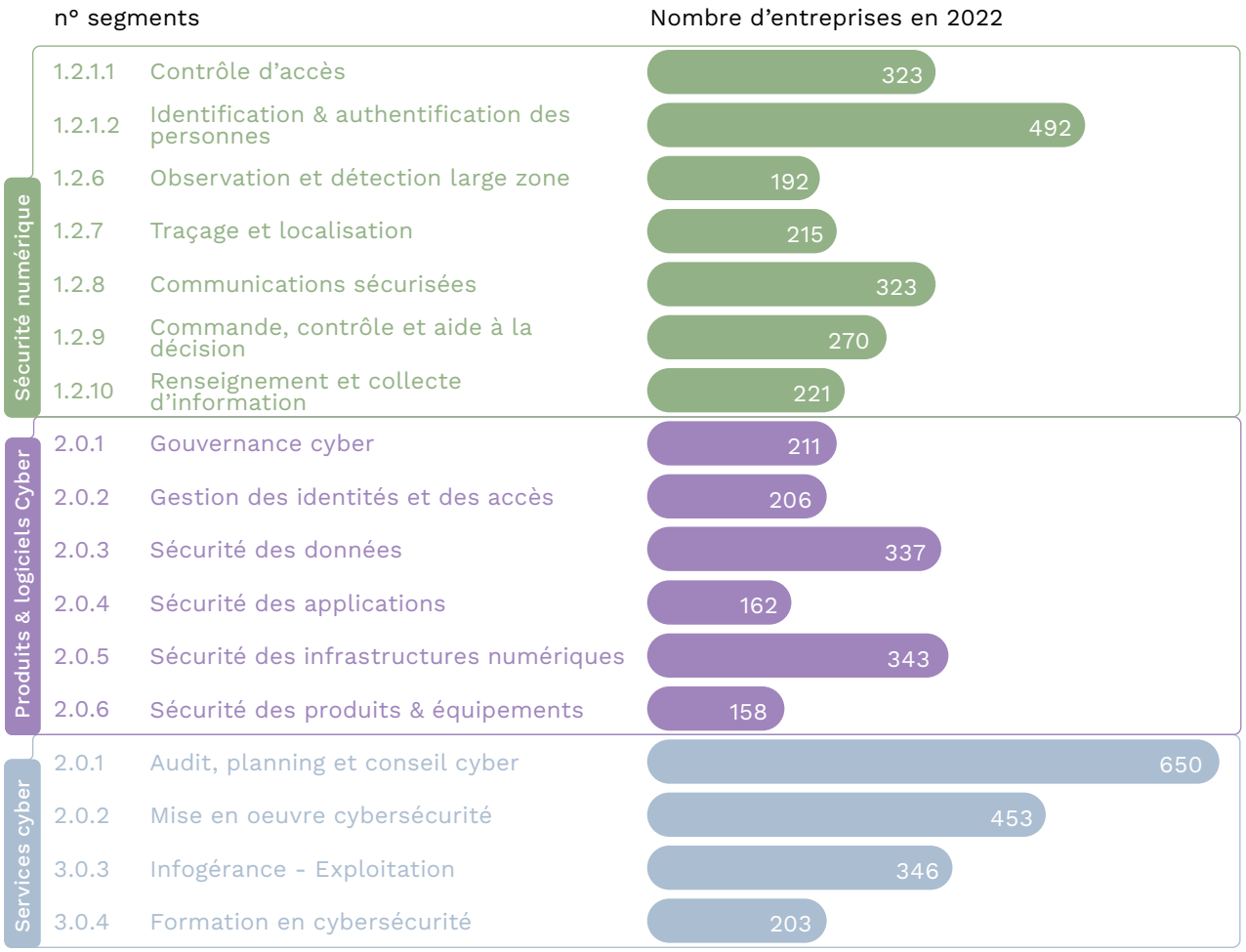


Sécurité Numérique	Poduits & logiciels Cyber	Services cyber	Total
34 771 emplois	+ 23 717 emplois	+ 28 257 emplois	= 86 745 Emplois de Confiance Numérique en France

Source : Decision Etudes & conseils

3.4 Nombre d'entreprises

Nombre d'entreprises en France en 2022 par segment



Sécurité Numérique	Poduits & logiciels Cyber	Services cyber	Total
1 741 entreprises	+ 703 entreprises	+ 690 entreprises	= 2 129 Entreprises de Confiance Numérique en France

Source : Decision Etudes & conseils

3.5 Les mouvements de fusion - acquisition

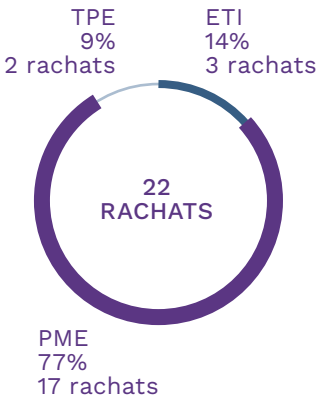
Bilan des rachats d'entreprises sur la période 2021-2023

Au sein de la filière de la Confiance Numérique, **41 rachats d'entreprises** concernant des sièges d'entreprises localisés en France ont été recensés de janvier 2021 à mars 2023 (soit en moyenne 17 rachats par an). Ces achats concernent aussi bien des achats inter-entreprises que des achats d'entreprises par des fonds financiers et des achats entre fonds financiers.

Parmi eux:

22 rachats d'entreprises françaises par d'autres entreprises françaises (54%)

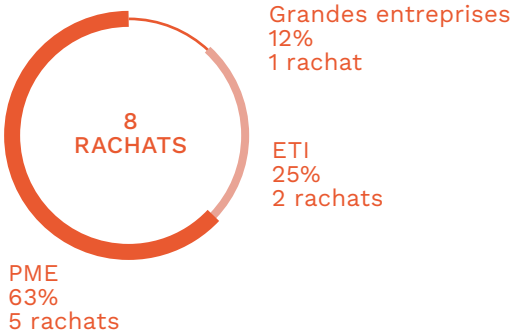
Rachats d'entreprises françaises par des entreprises françaises :



Source : Decision Etudes & conseils

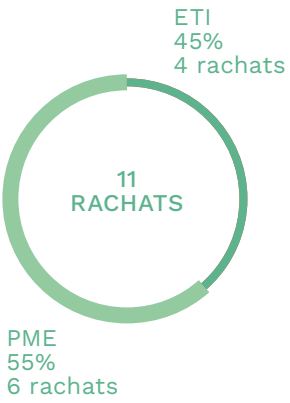
8 rachats d'entreprises françaises par des entreprises étrangères (19%)

Rachats d'entreprises françaises par des entreprises étrangères :



10 rachats d'entreprises étrangères par des entreprises françaises (27%)

Rachats d'entreprises étrangères par des entreprises françaises :



La grande majorité des entreprises rachetées sont des PME (68%) et des ETI (24%), en croissance.

Par rapport à la période 2017-2020, la fréquence de rachats est similaire, mais la taille des entreprises rachetées est en moyenne relativement plus petite, avec un fort attrait pour les PME.

En outre, sur la période 2017-2020, le nombre de rachats d'entreprises françaises par des capitaux étrangers était nettement supérieur au nombre de rachats d'entreprises étrangères par des entreprises de capitaux français, et pour des tailles d'entreprises achetées supérieures. **Cette tendance s'est estompée et même légèrement inversée depuis 2022.**

En 2021, les deux-tiers des rachats d'entreprises françaises par des entreprises étrangères se sont opérés au profit de capitaux américains, dans la continuité de la période 2017-2020. Parmi ces rachats, on trouve notamment Link by net, Openminded et AFD.TECH, tout les trois rachetés par Accenture. **En revanche, aucun rachat au profit d'entreprises américaines n'a été recensé en 2022.**

Enfin, les grands groupes français montrent leur intérêt pour le marché européen depuis 2022 en rachetant des entreprises dont le marché est généralement situé dans les pays frontaliers de la France.

A. Les principaux mouvements de l'année 2022 en France

ChapsVision et sa branche cyber Flandrin Technologies.

Le groupe français ChapsVision, éditeur de logiciels d'analyse de données, a connu une croissance rapide ces dernières années, avec pour objectif de devenir un acteur de référence dans le traitement massif des données. Depuis 2021, ChapsVision a réalisé plusieurs acquisitions stratégiques dans le secteur de la cybersécurité, renforçant ainsi sa position sur le marché et étendant considérablement ses activités. Parmi les dernières acquisitions de ChapsVision :

■ En 2021, rachat de Bertin IT et Vecsys à la CNIM, deux entreprises spécialisées dans les solutions logicielles de cyber intelligence, de veille stratégique, de traitement automatique de la parole et de cybersécurité. Grâce à ces acquisitions, ChapsVision prévoit de faire passer son chiffre d'affaires de 30 à plus de 40 millions d'euros et son effectif de 260 à 380 collaborateurs. Cette double opération s'inscrit dans la stratégie du groupe visant à capitaliser sur la protection des données.

■ Fin décembre 2021, rachat d'Elektron, filiale de Nexa Technologies (partenaire historique du ministère de la Justice, fournissant des solutions d'interceptions judiciaires). Suite à cette acquisition, ChapsVision créée sa branche dédiée aux activités cyber, nommée Flandrin Technologies. L'objectif est de créer un acteur souverain et leader européen dans ce domaine. Flandrin Technologies regroupe dès lors Bertin IT, Vecsys et Elektron.

■ Fin 2022, acquisition de Deveryware, financée par une levée de fonds de 100 millions d'euros, menée par Bpifrance et Tikehau Ace Capital. Deveryware est un leader des technologies d'investigation et services pour la sécurité globale. L'objectif de cette acquisition est de consolider la position de ChapsVision dans la cybersécurité et les technologies d'investigation, tout en proposant des services aux entités étatiques. Deveryware sera rattaché à Flandrin Technologies, portant ainsi le chiffre d'affaires du groupe à 100 millions d'euros et son effectif à 500 collaborateurs.

Ces acquisitions sont les exemples les plus notables parmi les 10 rachats que ChapsVision a réalisés dans le secteur de la cybersécurité depuis sa création en 2019. L'objectif de l'entreprise via sa branche Flandrin Technologies est de réaliser 250 millions d'euros de chiffre d'affaires d'ici 2024.

Grâce à une stratégie d'acquisition ciblée et ambitieuse, ChapsVision est en passe de devenir un acteur majeur de la filière cyber. Le groupe continue de renforcer sa position sur le marché et de consolider son expertise dans les technologies d'investigation, de cybersécurité et de traitement des données massives.

Sopra Steria acquiert CS Group pour 283 M€ et devient le numéro 5 de la filière en France.

Sopra Steria, leader européen des services numériques et de l'édition de logiciels, a annoncé le rachat de 75% du capital à termes de CS Group, spécialiste des systèmes critiques et de la cybersécurité. Cette acquisition stratégique vise à positionner les deux entreprises parmi les nouveaux champions de la cybersécurité.

L'acquisition de CS Group permettra à Sopra Steria de renforcer sa position sur le marché de la cybersécurité et de profiter de synergies importantes en termes d'expertise technique et métier afin de mieux répondre aux enjeux de sécurité et de Confiance Numérique auxquels font face les entreprises et les organisations publiques.

Docaposte rachète les activités de signature électronique et de coffre-fort numérique d'Idemia.

Début 2022, Docaposte a procédé à l'acquisition des activités de signature électronique et de stockage sécurisé d'Idemia, un acteur de référence de l'identité numérique et de la biométrie. La valeur de ces activités acquises s'élèverait à 57 millions d'euros selon nos estimations et permet à Docaposte de consolider sa position de numéro 1 français de la signature électronique, en enrichissant sa gamme de solutions de confiance avec une nouvelle brique technologique de stockage numérique pour les marchés réglementés.

B) Les principaux mouvements de l'année 2022 en Europe

Thales rachète S21sec et Excellium au portugais Sonae Group pour un montant de 120 M€.

S21sec et Excellium sont deux acteurs majeurs du conseil, de l'intégration et des services managés de cybersécurité en Europe. Par cette acquisition, Thales accélère l'exécution de sa feuille de route en matière de cybersécurité et renforce sa présence en Espagne, au Portugal, au Luxembourg et en Belgique. S21sec et Excellium emploient au total 546 personnes pour un chiffre d'affaires combiné de 59 millions d'euros en 2021. Cette acquisition vient compléter le portefeuille de Thales en cybersécurité, en renforçant ses services de détection d'incident et de réponse (Security Operations Centre – SOC) ainsi que ses prestations de conseil, d'audit et d'intégration.

Sopra Steria acquiert Tobania un spécialiste belge des services dans le numérique.

En novembre 2022, Sopra Steria a annoncé le rachat de la société de conseil et de services dans le numérique Tobania. Créée en 2014 à la suite de la fusion de deux sociétés, Saga Consulting et Tobius, cette entreprise belge compte 650 salariés pour un chiffre d'affaires de 110 millions d'euros.

Orange Cyberdefense acquiert les sociétés suisses SCRT et Telsys.

SCRT est une société spécialisée dans les audits et les tests d'intrusion, les SOC, le conseil et l'intégration de solutions tandis que Telsys, créée en 1989, est une entreprise positionnée sur le secteur des infrastructures réseaux, du cloud et des datacenters. Grâce à ce double rachat, Orange renforce son expertise en *threat intelligence* ainsi qu'en hacking éthique. Les montants financiers de l'opération ne sont pas communiqués.

Airbus renforce ses capacités de cryptographie et améliore le développement de systèmes sécurisés de bout en bout.

DSI Datensicherheit GmbH (DSI DS) est une société allemande qui fournit des systèmes de cryptographie et de communication pour les domaines Air & Espace, Mer et Terre, certifiée par l'Office fédéral de la sécurité de l'information (BSI). Cette acquisition fait suite à un partenariat de longue date entre les deux sociétés. DSI DS est entièrement détenue par Airbus Defence and Space et opère sous un nouveau nom, Aerospace Data Security GmbH. Cela renforce les capacités de cryptographie d'Airbus et améliorera le développement de systèmes sécurisés de bout en bout. Les termes du contrat n'ont pas été dévoilés.

3.6 Une année dynamique pour les levées de fonds

Signe de l'attractivité de la filière, les levées de fonds des startups de la Confiance Numérique voient **leur nombre et leur montant croitre de façon exponentielle depuis 5 ans.**

Comme le montre l'infographie ci-dessous, 21 levées de fonds ont eu lieu en 2020, 28 en 2021, 39 en 2022 et 6 au cours des trois premiers mois de 2023, dépassant déjà le montant des levées en 2020.

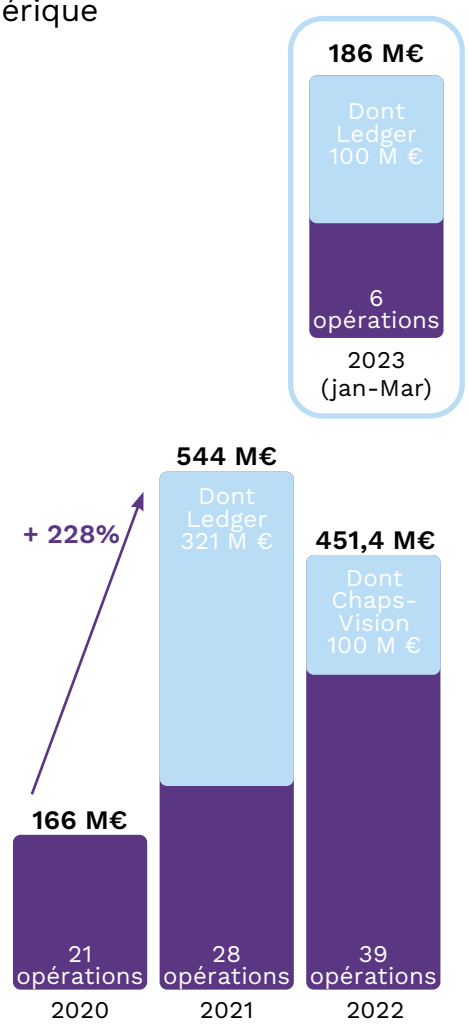
La filière a connu trois levées de fonds aux montants exceptionnels en trois ans : 321 millions d'euros pour Ledger en 2021, 100 millions d'euros pour Chapsvision en 2022 (servant en particulier à l'acquisition de Deveryware), et de nouveau Ledger avec 100 millions d'euros en mars 2023. En excluant ces levées aux montants exceptionnels, **les montants des levées de fonds n'ont cessé de croître, atteignant en 2022 plus du double du montant de 2020.**

Parmi les levées de fonds recensées en 2022, sur un montant global de 351,4 millions d'euros, hors ChapsVision, les membres de l'ACN représentent 40% des investissements, soit 140 millions d'euros. Parmi les principaux acteurs français derrière ces levées de fonds, on trouve la BPI, Tikehau Ace Capital, Jolt Capital, Elaia, Move Capital, Alliance entreprendre, Seventure Partners...

La France figure parmi les premiers pays en Europe en matière de levées de fonds de Confiance Numérique: **en deuxième position en nombre de levées et en troisième position en termes de montants levés.** Cette position est d'autant plus significative pour la filière et pour la France puisque selon le baromètre européen des investissements en cybersécurité réalisé en 2023 par Tikehau Ace Capital, l'Europe enregistre une baisse dans les levées de fonds tous secteurs confondus entre 2021 et 2022 tandis que la cybersécurité, malgré une légère baisse du nombre de levées, confirme sa croissance en montants levés.

Selon ce même baromètre, bien que la majorité des plus grosses levées de fonds dans le monde reste nord-américaine, la Suisse enregistre une année record avec 2 levées figurant dans le top 12 des plus importantes de 2022. Par ailleurs, le montant moyen levé aux États-Unis diminue, tandis que l'Europe consolide sa croissance de 2021 (avec une baisse de 39% aux États-Unis et une augmentation de 34% en Europe)

Montant des levées de fonds des startups française de la Confiance Numérique



Liste des levées de fonds des startups françaises de la Confiance Numérique

Levées de fonds en 2021

	Entreprise	Syndicat	Année	Montant (M€)
1	Ledger		2021	321
2	GuitGuardian		2021	39
3	Datadome		2021	30
4	Yousign		2021	30
5	Didomi		2021	29
6	YesWeHack	ACN	2021	16
7	Pr0ph3cy	ACN	2021	15
8	Glimps	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

Levées de fonds en 2022

	Entreprise	Syndicat	Année	Montant (M€)
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	

Levées de fonds en 2023

	Entreprise	Syndicat	Année	Montant (M€)
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 L'émergence d'un fort écosystème de PME de Confiance Numérique

Comme le montre l'infographie ci-contre, l'écosystème français de la Confiance Numérique s'est construit autour de grands acteurs historiques, souvent issus de la sécurité numérique et/ou des services numériques, et souvent liés aux écosystèmes régaliens et de défense. Ces grands acteurs historiques, fortement exportateurs, ont des offres orientées vers les états, les Opérateurs d'Importance Vitale (OIV), et les grandes entreprises internationales. Ils représentent 15,3 Mds € de chiffre d'affaires en 2022.

Cependant, un écosystème de PME spécialisées dans la Confiance Numérique a commencé à émerger à partir des années 1990. Au cours de la décennie des années 2010, **cet écosystème a progressivement pris de l'importance** et recense désormais de nombreuses grandes PME dont certaines ont déjà dépassé la barre des 50 M € de CA et sont devenues des Entreprises de Taille Intermédiaires (ETI), tournées vers l'international.

Cet écosystème est composé très majoritairement de startups de la cybersécurité dont beaucoup ont des offres visant à adresser de nouveaux marchés comme les PME/TPE ou encore les petites collectivités territoriales. **La forte croissance de cet écosystème est portée par des levées de fonds pour des montants toujours plus importants d'années en années.** Cet écosystème représente un chiffre d'affaires estimé entre 2 et 2,5 Mds € en 2022 (en additionnant les PME avec un chiffre d'affaires supérieur à 5 M €, les entreprises ayant bénéficié d'une levée de fonds pour un montant égal ou supérieur à 5 M € et les PME qui sont devenues des ETI depuis les années 2000).

Remarque : Les entreprises dont le logo est présent dans l'encadré sur l'écosystème des PME correspondent aux plus remarquables : Les ETI, les entreprises ayant bénéficié des plus grandes levées de fonds ou les PME avec les plus grands chiffre d'affaires.

Emergences d'un fort écosystème de PME

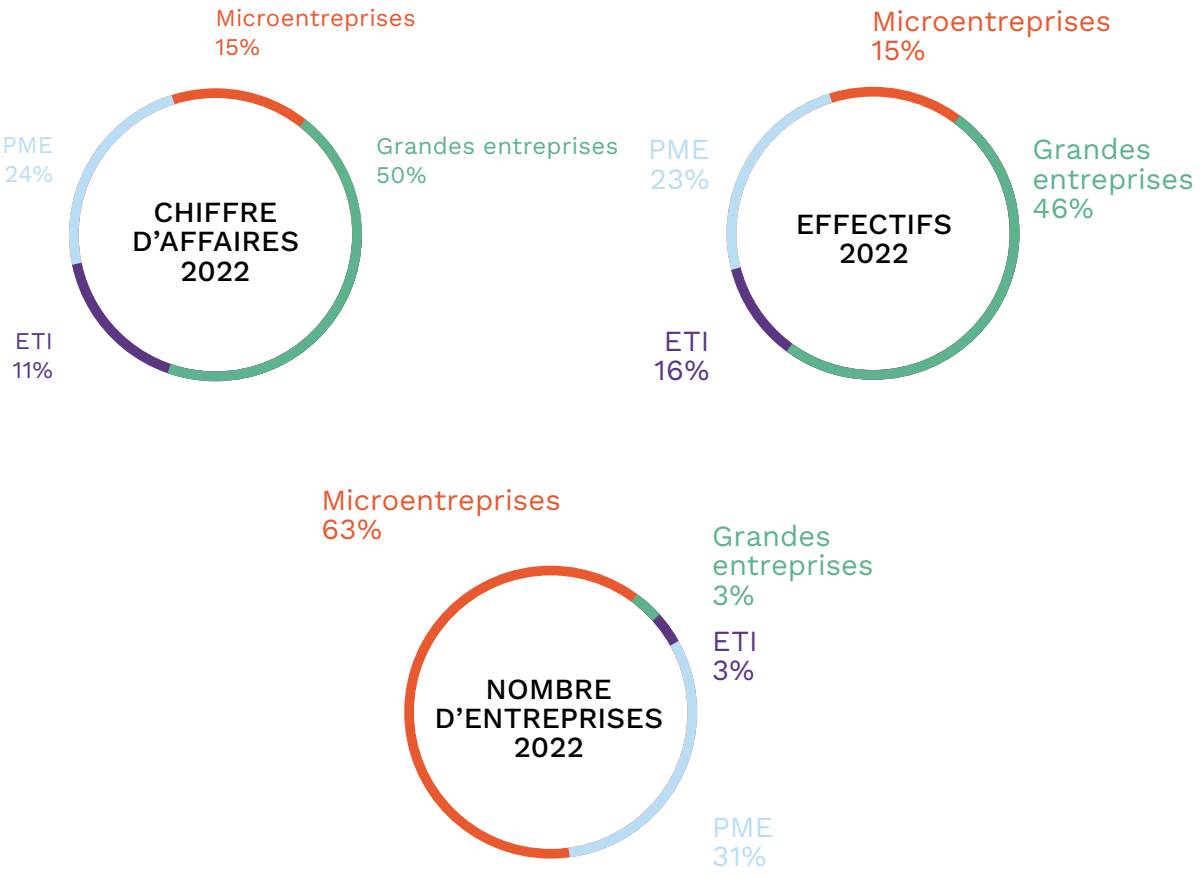
2,5 à 3 Mds € en 2022

nameshield · CHAPSVISION · CROSSCALL · NEOSOFT · nomios · APIXIT · i-TRACING · ZAMA · vade · AMOSSYS · WALLIX · yousign · ChamberSign · CybelAngel · CrowdSec · Systancia · stoïk · GATEWATCHER · verimatrix · alternativ.io · DATADOME · ARIADNEXT · Advanced Track & Trace · Ledger · egidium TECHNOLOGIES · NXO NEXTIRAONE · Citalid · CHEOPS TECHNOLOGY · sekoia · cogelec · SECURE-IC · squad · GitGuardian · MAILINBLACK · cozdrive · TEHTRIS · 123CS · WAVESTONE · yogosha

Grands acteurs historiques

15,3 Mds € en 2022

Analyse par taille d'entreprise



IV. POINT SUR LA MENACE INFORMATIQUE

4.1 La menace vue par l'ANSSI

Dans son Panorama de la cybermenace 2022, l'ANSSI (Agence Nationale de la Sécurité des Systèmes d'Information) revient sur les grandes tendances observées sur l'année 2021-2022 et en propose des perspectives d'évolution à court terme.

Avec un niveau général qui reste élevé, l'ANSSI constate que cette menace touche de moins en moins d'opérateurs régulés et se déporte sur des entités moins bien protégées. Si le nombre d'attaques par rançongiciel portées à la connaissance de l'ANSSI a diminué, la menace **d'espionnage informatique** demeure prégnante, ayant de nouveau fortement mobilisé les équipes de l'agence.

Evolution :
baisse de 23,2% des intrusions avérées

2021 :
1082 intrusions avérées

2022 :
831 intrusions avérées

Attention - Si le nombre d'intrusions avérées est en baisse, les conséquences des cyberattaques sur la période 2021-2022 sont tout aussi graves voire plus importantes encore.

Document de Référence :
Panorama de la Cybermenace 2022
ANSSI – 10 février 2023

Document disponible ci-dessous :
https://www.ssi.gouv.fr/publication/un-niveau-eleve-de-cybermenaces-en-2022/

1. Un niveau de menace général toujours élevé, en particulier pour les acteurs les moins bien protégés

La cybermenace n'a pas connu de grandes évolutions, **les tendances identifiées en 2021 se confirment en 2022.** Cependant, même si le nombre d'intrusions avérées est en baisse, les conséquences des cyberattaques sur la période 2021-2022 sont tout aussi graves voire plus importantes encore.

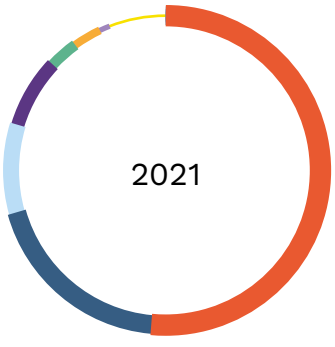
L'ANSSI précise qu'en début d'année 2022, le nombre d'intrusions avérées a baissé de 46% **mais qu'elles se sont réintensifiées à l'été 2022**, notamment vis-à-vis des collectivités territoriales et locales et les établissements public de santé.

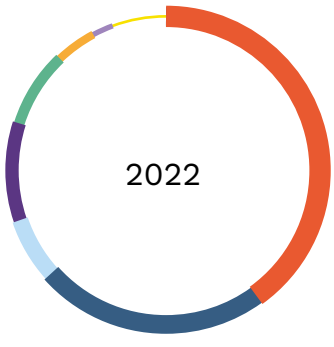
Aussi, le conflit russo-ukrainien a modifié l'écosystème des cybercriminels, certains groupes russophones ayant réorienté leurs ciblages afin de s'aligner sur les intérêts russes en Ukraine comme le groupe Conti. A l'inverse, certains cybercriminels prennent la Russie pour cible tandis que d'autres restent concentrés sur des attaques purement lucratives.

Le secteur des entreprises privées de lutte informatique offensive offrant des espiogiciels reste également très actif.

Les graphiques ci-dessous montrent l'évolution des cibles visées par rançongiciel dans le cadre des incidents traités par l'ANSSI en 2021 et en 2022, qui est la cyberattaque la plus courante sur cette période :

Types de victimes de compromission par rançongiciel





- PME / TPE / ETI
- Entreprise stratégique
- Etablissement d'enseignement supérieur
- Ministère
- Collectivité territoriale / locale
- Etablissement public de santé
- EPA, EPIC
- Autre (association, infrastrusture de transport...)

Par conséquent, les attaques touchent de moins en moins les opérateurs régulés et se déportent sur les acteurs les moins bien protégés comme les TPE/PME/ETI, les collectivités territoriales/locales et les établissements publics de santé.

2. Une amélioration continue des capacités des acteurs malveillants poursuivant les mêmes objectifs que sur l'année 2021

La constante amélioration des capacités des acteurs malveillants relevée par l'ANSSI est visible notamment par les accès toujours plus discrets et pérennes aux réseaux de leurs victimes. Pour atteindre leurs objectifs, les acteurs malveillants menacent les équipements périphériques (pare-feu, routeurs, ...) ainsi que la chaîne d'approvisionnement dans sa globalité (prestataires, fournisseurs, sous -traitants, organismes de tutelle, ...).

Les objectifs principaux des attaquants restent, comme en 2021, le gain financier, l'espionnage et la déstabilisation. Les attaques par rançongiciel des **gouvernements du Monténégro** en août 2022, du Pérou et du **Costa Rica** en avril 2022 sont des exemples significatifs de tentatives de déstabilisation et ont eu de lourdes conséquences sur le fonctionnement de l'administration et les services publics numériques de ces pays. En effet, Cuba a déclaré l'état d'urgence juste après cette attaque.

En France, c'est l'espionnage informatique qui a le plus impliqué les équipes de l'ANSSI et comme en 2021, **la majorité des cas traités impliquait des modes opératoires associés en source ouverte à la Chine.** Durant le premier semestre 2022, l'ANSSI a notamment traité la compromission d'un système d'information du secteur de la défense susceptible d'intéresser un gouvernement étranger.

Dans le contexte du conflit russo-ukrainien, les activités de déstabilisation et d'espionnage via des tentatives de sabotage informatique contre les infrastructures critiques ont été nombreuses **mais restent limitées à l'espace géographique de l'Ukraine.** Cependant, l'évolution du conflit et les conséquences économiques qui en résultent appellent à une vigilance de l'ensemble des organisations, notamment dans le secteur de l'énergie.

En Europe et en Amérique du Nord, la déstabilisation s'est manifestée par des actions de défiguration de site internet ou par des opérations informationnelles par exfiltration de données et ont fait de nombreuses victimes. **Une recrudescence de l'hacktivisme y a également été observée en 2022.** Néanmoins, l'impact médiatique des actions entreprises était souvent disproportionné par rapport au niveau de compétences mises en œuvre et à l'impact réel sur le fonctionnement de leurs cibles. Les conséquences ont été limitées à l'indisponibilité de certaines ressources et à des atteintes à l'image des cibles.

3. Une menace difficile à caractériser avec de nouveaux modes opératoires (moyens)

La complexification de la cartographie des activités malveillantes est due à l'usage de modes opératoires attribués en 2022 à des acteurs différents qu'en 2021. **Désormais, l'usage de rançongiciels n'est plus attribué qu'aux cybercriminels, mais également à des acteurs étatiques.** Par exemple, l'Albanie a subi, dans le cadre d'une opération de déstabilisation, plusieurs attaques par rançongiciels et par *wipers* (des programmes malveillants visant à détruire les données présentes sur un système d'information) qui ont entrainé l'indisponibilité temporaire de plusieurs services numériques et de sites gouvernementaux.

Dans le même sens, de nouveaux programmes malveillants sont utilisés à des fins d'activités cybercriminelles et d'espionnage. C'est le cas par exemple de la porte dérobée modulaire DarkCrystal RAT mise en vente sur les forums russophones et composé d'un *stealer* (un programme malveillant qui collecte différents types d'informations avant de les transmettre à son opérateur) qui s'adapte aux objectifs de l'attaquant en ajoutant des modules d'enregistrement de frappe, collectes des identifiants enregistrés sur le navigateur web ou même des captures d'écrans.

Les principaux moyens recensés par l'ANSSI au cours de l'année 2021-2022 sont les suivants :

- Les attaques par déni de service distribué (DDoS),
- Les attaques par raçongiciel notamment par les groupes Avaddon, Bitlocker, Black Cat, Conti, Darkiside, Everest, Hive, LockBit, Mespinoza/Pyza, Phobos, Play, Ryk et Sodinokibi,
- L'arnaque par l'assurance maladie,
- La revente de données pour des campagnes d'hameçonnages crédibles,
- Les services de vente d'accès ou de programmes malveillants.

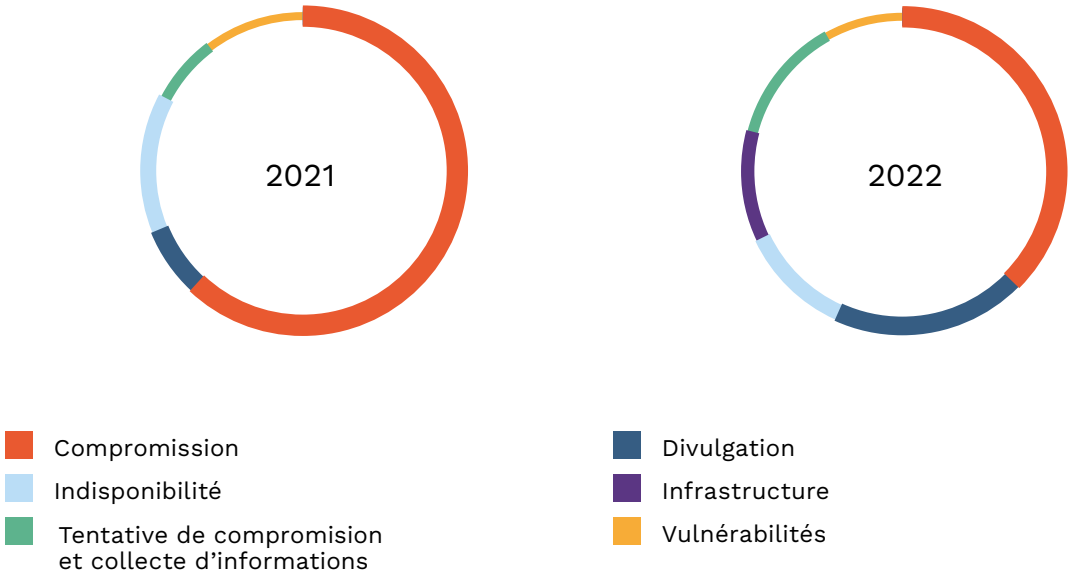
Le cryptominage est également utilisé afin de générer des fonds importants qui sont réinvestis par les acteurs malveillants afin d'acquérir de nouvelles capacités. Il est de moins en moins détectable car les attaquants parviennent à consommer de moins en moins de puissance de calcul sur les machines compromises ou en dissimulant les traces de leurs activités. Les infrastructures *cloud* peuvent notamment être exploitées à des fins de cryptominage.

Dans la même mesure, de nombreux incidents observés par l'ANSSI au cours de l'année 2022 ont pour origine **l'exploitation de vulnérabilités disposant de correctifs et ayant fait l'objet d'avis ou de bulletins d'alertes sur le site du CERT-FR.**

Enfin, en 2022, près de la moitié des opérations de cyberdéfense et les incidents majeurs traités par l'agence impliquaient de nouveaux modes opératoires associés en source ouverte à la Chine. En effet, les nouvelles technologies, les nouveaux usages, le *cloud computing* (une prestation de services informatiques sur Internet) et l'externalisation de services informatiques ont accru la surface d'attaque.

Comparatif des types d'incidents affectant les ESN

(entreprise de service numérique)



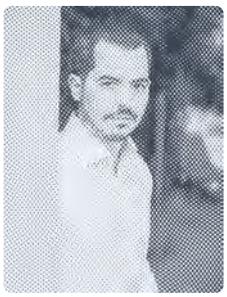
4.2 Regards croisés des experts du secteur

Révolution dans le vol d'identifiants

Erwan Keraudy
CEO

« Les emails piratés ont été la principale cause de fuites de données et de cyberattaques en 2022, et les nouveaux identifiants compromis augmentent de 45% annuellement. Les malwares de type *Infostealers* sont en train de prendre une ampleur considérable. Téléchargés à l'insu des utilisateurs, ces logiciels espions infiltrent les ordinateurs et exfiltrent dans le plus grand secret des informations sensibles comme des accès privilégiés à des réseaux informatiques ainsi que des données confidentielles et personnelles. CybelAngel détecte plus de 20 millions d'identifiants compromis chaque semaine. La menace va continuer à grandir et peser sur le paysage cyber en 2023, il est donc crucial de prendre des mesures de sécurité dès maintenant. »

Protéger son infra des menaces USB



Quentin Ruillere
Co-founder & CEO

« La clé USB qui introduit un *malware* dans le système d'information d'une entreprise est malheureusement un grand classique des cyberattaques. Entre les clés « *USBKiller* », «*Rookit* » ou *backdoor*, 30% des infections ont pour origine des supports USB et 40 % des clés USB contiendraient au moins un dossier présentant des risques. Si la sensibilisation des collaborateurs à ce risque est essentielle pour adopter les bons comportements, elle n'est pas suffisante. Selon l'ANSSI, seule une station blanche permet de prévenir tout risque d'infection. Il s'agit d'un poste dédié à l'analyse et à la gestion de périphériques USB (qu'il s'agisse de clés USB, de disques durs amovibles ou de lecteurs de DVD). Hogo est fier de proposer l'unique station blanche certifiée CSPN par l'ANSSI sur le marché. »

Vers des écosystèmes de données sûrs et souverains.

Julia Chaulet
CEO & co-fondatrice

« L'externalisation du stockage et du traitement des données voit ses limites exposées. Les géants du *cloud* sont loin d'être hermétiques au risque cyber et chacune de leur faille coûte cher à leurs clients : les nombreuses divulgations de données issues des serveurs AWS en sont une illustration directe. Le gouvernement et les entreprises françaises multiplient les actions pour sortir de cette dépendance technologique vis-à-vis des géants américains. Les initiatives telles que le visa de sécurité SecNumCloud ou le plan France 2030, favorisent les initiatives et innovations françaises pour répondre à ce défi. Dans ce contexte, l'essor des technologies de mutualisation des données sécurisées et souveraines est une nécessité pour garantir la croissance des entreprises françaises et européennes. »

La menace invisible des réseaux hybrides

Fanch Francis
CEO

« Les réseaux hybrides (*on-prem* et *cloud*, IT et OT, *core* et *edge*) se multiplient et décuplent les défis de cybersécurité. Superviser tous ses réseaux d'un point de vue unique est indispensable pour assurer une protection complète. NANO Corp propose une plateforme unifiée pour détecter et réagir aux cybermenaces sur ces réseaux. Les algorithmes d'apprentissage automatique et l'analyse comportementale permettent une détection précise des anomalies et une réaction automatisée aux incidents. Cette solution est nécessaire tant pour les SOC et NOC. Elle permet de garder le contrôle de sa surface d'attaque en prenant notamment en compte les machines non déclarées, orphelines ou non manageables, minimisant les risques de violation de données coûteuses et de dommages à la réputation. »

Une adoption croissante de l'authentification forte

Bruno Bernard
Président

« La sécurité des données numériques est essentielle face à la multiplication des cybermenaces. En 2022, plus de 51 types ont été gérés par la plateforme cybermalveillance.gouv.fr avec en tête l'hameçonnage ou *phishing*. Pour faire face à ce type d'attaques de plus en plus sophistiquées, la double authentification par SMS n'est plus suffisante. Pour une sécurité maximale, il est recommandé d'utiliser des moyens d'authentification forte tels que les dispositifs matériels FIDO. Le standard FIDO a été adopté par Microsoft, Google, Apple et plus de 150 fournisseurs de services parmi lesquels figurent les fédérations d'identité telles qu'Evidian, Ilex, Systancia, Octka, Ping Identity, ... »

La nécessaire montée en maturité des plus petites entités pour faire face à la cybermenace

François Esnol-Feugeas
CEO

« La menace *ransomware* a beau être en (léger) recul, elle reste le risque n°1 pour les entreprises, avec une actualité toujours très riche - le Centre Hospitalier Sud Francilien ou la Région Grand Est en sont des exemples parmi tant d'autres ! Cette menace touche particulièrement les plus petites entités, moins matures dans leur gestion du risque cyber. Le besoin d'une montée du niveau de protection de ces structures est donc critique, eu égard au risque fatal qu'elles courent quand aucun Plan de Reprise d'Activité (PRA) n'existe. Le besoin en solutions de cybersécurité simples à déployer et abordables, aussi bien techniquement que financièrement, n'a donc jamais été autant présent ! »

Une menace protéiforme qui continue à se professionnaliser

François Deruty
Chief Intelligence Officer

« 2022, année de la cyberguerre ? Résolument non : malgré une hausse des activités cyber dans la zone, la guerre en Ukraine n'a pas eu les effets escomptés dans le cyberespace. Mais pendant qu'on regarde du côté du côté russe, les acteurs APT sinophones sont de plus en plus offensifs en matière d'espionnage stratégique et économique... et ciblent la France. 2022 a aussi été l'année de la professionnalisation des *infostealers*, ces logiciels visant à voler des données personnelles. Comme pour les *ransomwares*, on observe une structuration de l'écosystème cybercriminel et le développement du "*as-a-service*". Ces évolutions confirment la nécessité pour les organisations de disposer de capacités de détection performantes, grâce à des renseignements précis sur les attaquants et leurs modes opératoires. »

TPE-PME : La prise de conscience est là, maintenant il faut agir

Léo Richer
CEO

« Les dirigeants des TPE et PME sont parfaitement conscients des risques liés à la cybersécurité qui pèsent sur leurs entreprises. Cependant, nombreux sont ceux qui choisissent d'ignorer le problème, convaincus que les solutions adéquates seraient trop onéreuses ou complexes à mettre en place. Il incombe au secteur de convaincre ces dirigeants que des solutions adaptées existent. Pour ce faire, il est essentiel de les sensibiliser et de les informer sur leur situation actuelle tout en leur proposant des solutions et des axes d'amélioration adaptés. L'ANSSI a donné la direction à suivre en prônant la nécessité de «massifier» la cybersécurité. Il est désormais temps de généraliser cette approche et de veiller à ce que les petites entreprises ne soient pas laissées pour compte. »

Notre perception de la menace résumée en 3 V : Vélocité, Volume, Variété

Laurent Oudot
CTO

« Nous avons analysé ces derniers mois des millions de menaces dans plus de 120 pays. Les tendances suivantes ont été identifiées :
•Les *ransomware* constituent toujours la principale menace, accompagnés de double extorsion (divulgation de données sensibles en cas de non-paiements des rançons) malgré un ralentissement au début de la guerre en Ukraine imposant une réorganisation des groupes de cybercriminels (pour ou contre la Russie).
•L'hameçonnage par courrier électronique, SMS et applications mobiles restent les moyens principaux d'obtention d'informations sensibles.
•Les attaques de *Supply Chain* et de l'IoT ont augmenté.
•Les opérations les plus dévastatrices ont utilisé des vulnérabilités des produits Microsoft (Windows, Office, Exchange, Active Directory) ou d'autres applications parfois trop exposées.

Les cyber défenseurs sont très bons, mais leurs moyens alloués ne sont parfois pas suffisants face aux menaces actuelles. »

Bruno Charrat
Adjoint à la directrice de la recherche technologique, CEA

Jean-Yves Marion
Directeur du Laboratoire lorrain de recherche en informatique et ses applications (LORIA)

Référent scientifique pour la filière cybersécurité du CNRS

La recherche française se mobilise face à la menace cyber

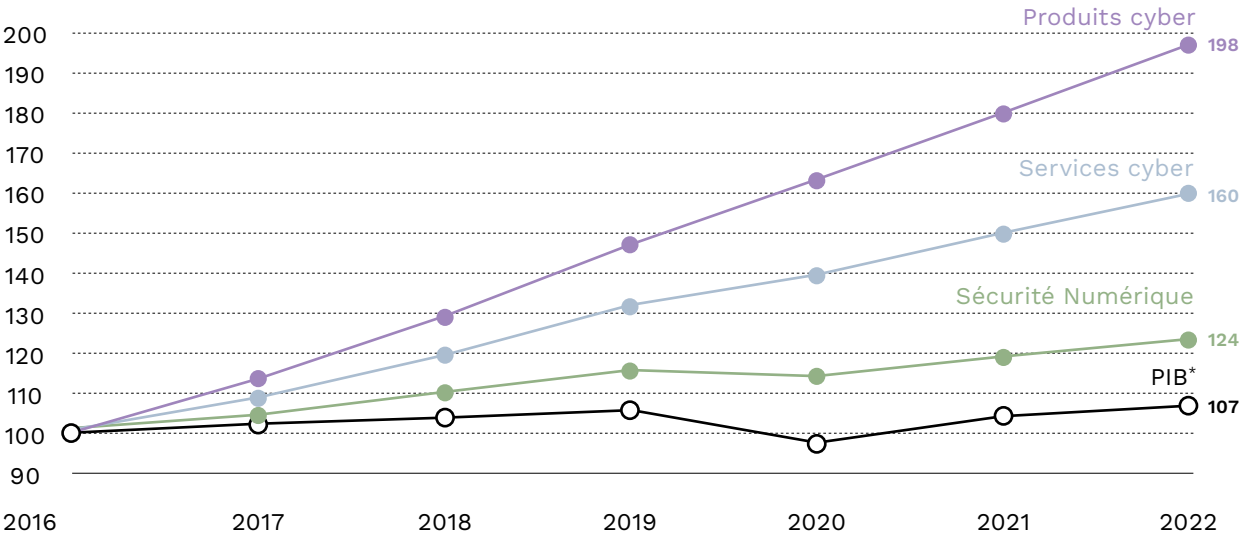
« Face à l'évolution rapide et constante de la menace cyber, il est plus que jamais essentiel de contribuer à la maîtrise de technologies numériques souveraines et sûres. La France dispose d'une communauté de recherche d'excellence en cybersécurité. La stratégie nationale pour la cybersécurité la mobilise dans des approches collaboratives et coopératives avec les acteurs socio-économiques et étatiques sur tout le continuum recherche fondamentale, innovation et entrepreneuriat. Son programme de recherche (PEPR) vise ainsi à apporter des réponses à dix défis de recherche fondamentale. Le Programme de Transfert du Campus Cyber (PTCC), plus axé sur la recherche appliquée et le transfert technologique, soutient également la formation et l'entrepreneuriat. Ces nouveaux outils permettent de structurer des communautés de recherche interdisciplinaires et au meilleur niveau mondial pour développer les technologies et outils indispensables à la filière et contribuer à une transition numérique sécurisée et résiliente pour les citoyens, les entreprises et les institutions. »

V. LES TENDANCES DE MARCHÉ

5.1 Les tendances générales

Le graphique ci-dessous montre l'évolution comparée de la croissance des trois principaux segments de la filière Confiance Numérique et du PIB sur la période 2016-2022.

Croissance France comparée 2017-2022



Croissance

Segments	2017	2018	2019	2020	2021	2022
Confiance numérique	**7,8 %**	**8,2 %**	**8,5 %**	**3,6 %**	**7,3 %**	**10,1 %**
Produits cyber	14,3 %	13,9 %	14,0 %	10,9 %	8,8 %	10,5 %
Services cyber	9,3 %	9,9 %	10,3 %	5,8 %	8,9 %	10,7 %
Sécurité Numérique	4,2 %	4,7 %	4,8 %	-1,7 %	5,2 %	9,4 %
PIB*	1,1 %	2,3 %	1,9 %	1,8 %	-7, %	6,8 %

*Source: INSEE, FMI pour l'année 2022

5.1.a. La croissance de la filière française

2021 : Une forte reprise post-COVID

En 2021, après une année 2020 marquée par la crise COVID, la filière de la Confiance Numérique a renoué avec une croissance forte de 7,2% portée par des tendances structurelles qui ont émergé il y a plus de dix ans et vont en s'accroissant d'année en année.

Principaux drivers de la croissance de la Confiance numérique :

■ **Accélération de la croissance « numérique »** portée par la crise sanitaire et les besoins accrus de connectivité. Le télétravail a notamment accru l'attention des entreprises autour des problématiques de cybersécurité (plateformes sécurisées de télétravail, etc.), de même que l'importance des paiements numériques devant être sécurisés.

■ **Accélération du déploiement de *clouds*** d'entreprises mais aussi de *clouds* applicatifs (*Continuum Cloud-to-Edge*), soutenant la demande d'un ensemble d'offres de Confiance Numérique autour des *clouds* de confiance, de la sécurité du *cloud* et de la sécurité *at-the-edge*. Ces tendances bénéficient particulièrement à des offres de produits cyber : gestion des identités et des accès (IAM), sécurité des données, sécurité des infrastructures et sécurité des produits et équipements (éléments sécurisés…).

■ **Augmentation continue des cyberattaques** (particulièrement les *ransomware* depuis plusieurs années). En outre, 75% des victimes de *ransomware* sont désormais des petites et moyennes entreprises qui manquent de ressources dédiées (*Orange Cyber Security Report*, 2021). Le marché de protection des PME et TPE françaises est à ce titre très prometteur. En 2023, le *Security Navigator Report* d'Orange note cependant pour la première fois un ralentissement de la croissance des cyberattaques.

La baisse tendancielle de la croissance de la cybersécurité

Depuis 2018, on observe une baisse tendancielle de la croissance de la filière de cybersécurité. Cela tient simplement au fait que **ce secteur commence à atteindre une taille conséquente avec près de 10 Mds € réalisés depuis la France en 2022.** La croissance se poursuit donc, mais les taux de croissance relatifs à la taille du secteur vont progressivement baisser en dessous de la barre des 10%. Signe de la très forte croissance de ce segment, **le chiffre d'affaires généré en France par les produits cyber a doublé en 6 ans (entre 2016 et 2022).**

Une croissance particulièrement forte en 2022, portée par la sécurité numérique

L'année 2022 est marquée par une croissance particulièrement forte. La cybersécurité réalise une bonne année avec 10,6%, légèrement en dessous de la tendance des années 2014-2019.
Cependant, la sécurité numérique réalise une année exceptionnelle avec une croissance de 9,4%. Cette croissance a trois facteurs explicatifs :

La subsistance d'un effet rebond suite à la période de récession associée à la crise du COVID (près de -2% en 2020, certains grands acteurs ayant connu une récession jusqu'en 2021).

La répercussion de la hausse des prix des semi-conducteurs suite à la pénurie mondiale, induisant une croissance en valeur. Cela est particulièrement vrai pour le segment de l'identification et authentification des personnes (cartes à puces,…) et pour le segment cyber de la sécurité des équipements (éléments sécurisés, HSM), mais ce phénomène s'étend à l'ensemble de la sécurité numérique.

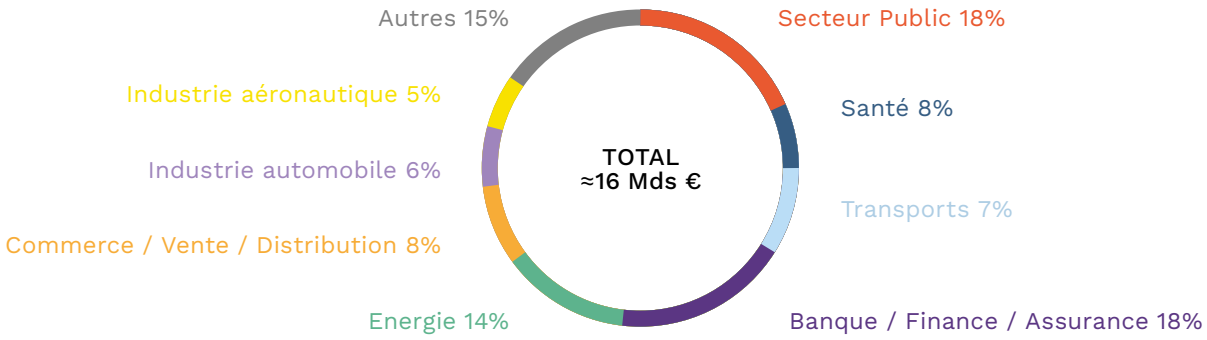
Enfin, **une conjoncture favorable induisant une croissance en volume :** importance croissante de l'enjeu du contrôle aux frontière avec des projets publics qui se multiplient, augmentation de la demande sécuritaire des États européens en lien avec la guerre en Ukraine, sécurisation des grands évènements (Coupe du monde de rugby en France en 2023, JO de Paris en 2024…).

5.1.b. Les marchés de la filière en 2022

Comme le montre le diagramme ci-dessous, le **secteur public au sens large,** c'est-à-dire en incluant les transports et la santé **représente un tiers du marché français** (5-6 Mds € en 2022), **les deux tiers restants provenant du secteur privé** (10-11 Mds €).

Le poids du secteur privé est appelé à croitre d'année en année. La filière de la Confiance Numérique est en effet née autour de l'Etat et du besoin de sécurisation des Opérateurs d'Importance Vitale (OIV). Le besoin de confiance s'est ensuite étendu aux grandes entreprises en général, au-delà des OIV. La tendance actuelle est désormais au développement du marché des PME et TPE, qui sont pour la plupart démunies face au risque de cyberattaques qui les concerne désormais, en particulier le risque de subir un rançongiciel.

Principaux marchés de la filière en 2022



Source: DECISION Etudes & Conseil, questionnaire renseigné par les entreprises de la filière.

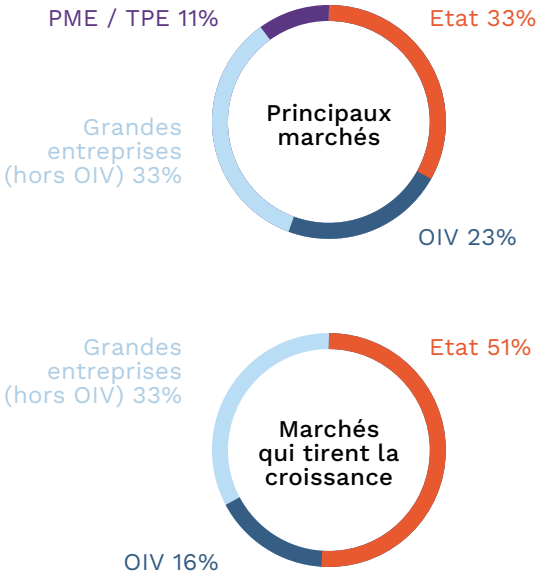
Pour l'année 2022, le secteur public continue cependant d'être indiqué comme l'un des premiers moteurs de la croissance par les entreprises de la filière ayant répondu à notre questionnaire, au côté du secteur Banque / Finance / Assurance et du secteur de l'énergie.

L'émergence d'un marché des PME/TPE et des petites collectivités territoriales

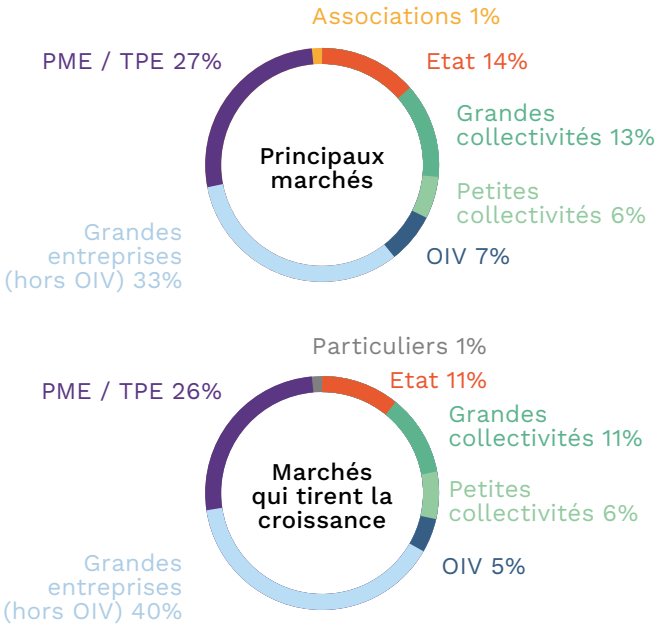
La série de diagrammes ci-contre, issue de l'édition 2023 du questionnaire en ligne auprès des acteurs de la filière, montre la segmentation du marché français de la filière selon le type d'entreprise fournisseur de solutions de confiance (grande entreprise versus PME/TPE).

On observe que l'Etat, les Opérateurs d'Importance Vitale (OIV) et les grandes entreprises (hors OIV) représentent près de 90% du marché des grandes entreprises de la filière, et près de 100% de leurs perspectives de croissance pour les années à venir. Ces grandes entreprises fournisseurs de solutions de confiance représentent 50% du chiffre d'affaires de la filière en France en 2022 (65% si l'on inclut les activités réalisées hors de France). On retrouve donc ici les grands marchés traditionnels autours desquels la filière s'est construite : Etat, OIV et grands comptes privés.

Grandes entreprises



TPE / PME



A contrario, l'Etat et les OIV ne représentent que 21% du marché des PME et TPE de la filière. Ce sont les grandes entreprises (33%), les PME / TPE (27%) et les collectivités locales (19%) qui représentent l'essentiel du marché et des perspectives de croissance pour les PME et TPE fournisseurs de solutions de confiance en France. Autrement dit, à travers cette vision des PME et TPE de la filière, on observe l'émergence de deux marchés :

■ **Celui des collectivités locales,** y compris les petites collectivités locales. Par extrapolation, on peut estimer le marché des petites collectivités locales entre 800 millions d'euros et 1 milliard d'euros en 2022.

■ Mais surtout, **le développement du marché associé au besoin de produits et services de confiance de la part des PME et TPE françaises.** Par extrapolation, on peut estimer ce marché entre 3,5 et 4,5 milliards d'euros en 2022. Ce marché se caractérise par des offres dédiées : offre standardisée, déploiement rapide, faible coût, souvent sans support *hardware*...

Le développement de ce marché des PME et TPE françaises a été ralenti en 2020 par la crise du COVID. En effet, les PME et TPE françaises ont été plus affectées par les restrictions associées au COVID que les grands clients traditionnels de la filière de la Confiance Numérique (Etat, OIV, grandes entreprises) qui sont quant à eux particulièrement centrés sur la fourniture de besoins essentiels (Banque / Finance / Assurance, Energie, Santé...).

Cependant, la tendance structurelle est bien au développement de ce marché des PME et TPE qui est voué à devenir l'un des grands marchés de la filière et va sous-tendre sa croissance pour les années à venir.

Focus JO - Sécurisation des JOP 2024

EXPÉRIMENTATIONS POUR LA SÉCURISATION DES JOP 2024 : UNE RÉUSSITE COLLECTIVE QUI TÉMOIGNE DU DYNAMISME DE NOTRE INDUSTRIE.

Gérard Lacroix
(GICAT), Délégué général adjoint à la sécurité

Depuis avril 2022, le Conseil Stratégique de Filière des Industries de Sécurité (CSF-IS) mène en coopération avec le ministère de l'Intérieur et des Outre-mer un vaste programme d'expérimentations technologiques, dans le cadre d'un travail collectif et ambitieux engagé dès 2018 pour proposer un plan global de sécurité des grands événements. Structuré depuis la mi-2019 autour d'un groupement d'industriels chefs de file (Airbus, Atos, Idemia, Orange et Thales) matérialisé par la Proposition globale de sécurité « Grands événements et Jeux Olympiques et Paralympiques Paris 2024 », le CSF-IS a mené, au travers de son programme d'expérimentations innovant et original, la réussite d'une initiative inédite. Sous l'impulsion de Gérard Lacroix (GICAT) et de Daniel Le Coguic (Atos), elle a rassemblé pouvoirs publics et industries autour de quatre objectifs principaux : garantir la sécurité et l'esprit festif des Jeux, améliorer substantiellement les capacités des forces de sécurité intérieure, fédérer l'industrie française de la sécurité et en faire un champion international et contribuer à l'héritage du programme olympique tout en développant un modèle exportable.

Axé sur un ensemble de thématiques structurantes et incontournables pour les forces de sécurité intérieure et de secours françaises, telles que les centres de commandement, le renseignement, la cybersécurité, la lutte anti-drone, la vidéo protection, la gestion des foules ou encore la défense NRBC, ce programme a permis l'inclusion de l'ensemble des acteurs de la filière en particulier les PME/PMI et start-ups innovantes. Largement relayée et ouverte à tous, au travers d'appels à manifestation d'intérêt (AMI), la démarche a permis l'analyse de près de 700 solutions issues de 171 sociétés différentes, témoignant ainsi de la richesse de l'écosystème industriel français. A l'issue de ces AMI, près de 200 solutions ont pu être expérimentées grâce à la mobilisation de 89 sociétés différentes. Les résultats sont inédits et vont bien au-delà des objectifs d'inclusion et de souveraineté initialement fixés et pris par le CSF-IS puisque 90% des solutions testées étaient françaises (objectif initial à 80%) et que 75% de ces solutions étaient issues de start-ups, PME/PMI ou ETI (objectif initial à 30%). Les adhérents du GICAT ont, pour leur part, participé très activement sur 45% des solutions expérimentées.

Ce formidable investissement de la filière est donc une belle réussite collective de mise en place de technologies souveraines et témoigne du dynamisme de notre industrie.

Alors que s'achève cette phase de mobilisation sans précédent des industriels français de la sécurité, le CSF-IS tire de ce programme un ensemble de conclusions qu'il a partagées avec le ministère de l'Intérieur et des Outre-mer et les forces de sécurité. A ce titre, des plans d'acquisitions substantiels conformes à la Loi d'orientation et de programmation du ministère de l'Intérieur de janvier 2023 (LOPMI) devraient être mis en application dans les domaines des centres de commandement, la cybersécurité, la vidéo protection, la lutte anti-drone, le renseignement et la surveillance intelligente des frontières. Dans la perspective du deuxième contrat de filière, il semble désormais opportun et pertinent d'étendre ce programme générateur de valeur aux autres composantes du continuum de sécurité, aux collectivités territoriales, aux OIV et aux OSE. Cette démarche pourrait se matérialiser par de nouveaux programmes d'expérimentation, la mise en place d'instances conjointes (laboratoire d'innovation) ou, de manière plus ambitieuse encore, la structuration de programmes d'exports (Milan 2026, CDM FIFA 2026, Los Angeles 2028...).

C'est quoi la LOPMI ?

Particulièrement attendue, la LOI n° 2023-22 du 24 janvier 2023 d'orientation et de programmation du ministère de l'Intérieur (LOPMI) fixe, pour les cinq ans à venir, les objectifs prioritaires en termes de politiques publiques de sécurité parmi lesquels la prévention du terrorisme, la lutte contre le trafic de drogue et la répression des violences intrafamiliales, notamment. Sur le plan budgétaire, la loi prévoit 15 milliards d'euros de crédits supplémentaires. Le ministère de l'Intérieur pourra ainsi poursuivre sa modernisation, a fortiori dans le domaine du numérique : démarches dématérialisées, outils de travail en mobilité, moyens d'investigation modernisés, etc. Enfin, le renforcement du continuum de sécurité prévu par la LOPMI, est une garantie de mobilisation de l'ensemble des acteurs, publics comme privés, au profit de la sécurité générale de la Nation, notamment dans la perspective des Jeux olympiques et paralympiques de Paris, en 2024.

Histoire | Les JOP2024 sont exceptionnels par leur ampleur et leur durée

Pour illustrer le caractère exceptionnel de l'événement, un chiffre à retenir : plus de 12 millions de visiteurs venus du monde entier sont attendus. A titre d'exemple, les Jeux Olympiques (26 juillet au 11 août) peuvent être comparés à environ 46 coupes du Monde de Football. Les Jeux Paralympiques, eux, auront lieu du 28 août au 8 septembre.

Quelques chiffres clés sur cet événement :

- **12 millions** de spectateurs
- **8 millions** de fans sur les live sites
- **20 000** Journalistes accrédités
- **17 000** athlètes
- **70 000** volontaires
- **15 millions de personnes** sur le parcours de la flamme
- **4 milliards** de téléspectateurs
- **100 000 heures** de diffusion TV
- **68 500** Personnels de sécurité

Source : annexe technique de sécurité PARIS2024 / 2: Avec sites d'entrainements etc (CNSJ)

Menaces | Le niveau des menaces autour de la Coupe du Monde de Rugby 2023 et des JOP2024 obligent à renforcer la posture cybersécurité du ministère de l'Intérieur

L'incidentologie attendue, liée aux attaques d'origine cyber, sera extrêmement élevée et atteindra un pic pour les JOP2024. Les attaques risquent de cibler principalement le Comité d'Organisation des Jeux Olympiques (COJO), dans un objectif de perturber mais également par appât du gain. Infrastructures de diffusion des Jeux, cérémonie d'ouverture, moyens de communication physiques et en ligne, autant de menaces qu'il convient d'anticiper.

Un niveau de la menace favorisée par un contexte exceptionnel
Les flux importants de personnes avant et pendant ces évènements et la diffusion en direct de l'événement nécessiteront un niveau de vigilance élevé, en particulier dans un contexte géopolitique actuellement tendu et un hacktivisme virulent (religieux, écologique,...). La France sera en effet le cœur du monde pendant ces quelques semaines.

Les profils d'attaquants sont divers ; on retrouve ceux sponsorisés par des gouvernements étrangers disposants de moyens d'attaque illimités pour atteindre des cibles stratégiques, des criminels motivés par les demandes de rançons ou les hacktivistes adeptes du défacement de site web, par exemple.

Enjeux | La sécurité des grands évènements en France représente des enjeux et des opportunités pour l'industrie

La sécurisation des JOP2024 revêt un intérêt stratégique pour la France. Elle constitue une opportunité de réussite, de structuration et de valorisation de notre filière industrielle. Tous les acteurs aspirent à préserver l'esprit festif des jeux et à laisser une place significative aux citoyens, tout en maîtrisant les coûts et limitant les effectifs. Au travers de la constitution d'un écosystème intégrant PME/PMI, ETI, startups, c'est toute la filière sécurité qui se mobilise.

Cette opportunité se justifie par la possibilité de voir, à l'issue, de nombreux retours sur investissements. Elle constitue un accélérateur pour la modernisation des moyens actuels de la sécurité publique et la montée en compétence des personnels de sécurité privée et publique, tout en étant créatrice d'emplois pour la filière. Accompagnée par une évolution du cadre légal, amorçant une rupture technologique contrôlée, elle saura mettre en lumière la France et son écosystème riche et diversifié autour d'une filière d'excellence qui favorisera l'export du savoir-faire français à l'international.

CSF-IS | le Conseil Stratégique de Filière des Industries de sécurité (CSF) est engagé auprès du ministère de l'Intérieur

Groupe Mixte

Comité de pilotage mixte
Rendre compte de l'état d'avancement des travaux et valider les orientations
Intégration des AMI

Atelier de Design Thinking
Affiner les analyses des risques, les expressions de besoin et l'évolution des dispositifs de sécurité
Prise en compte des travaux du COFIS

Groupe de travail et séminaires mixtes
Evaluation des technologies et de leurs impacts, retours d'expérience des opérationnels de sécurité
Analyse des plans de sécurité existants

Entre juillet et novembre 2019, le CSF-IS a donc œuvré en co-construction avec l'Etat à la rédaction de **quatre documents** phares, répondant à **quatre objectifs majeurs** :

1. Garantir la sécurité et l'esprit festif des Jeux ;
2. Améliorer substantiellement les capacités des forces de sécurité intérieure ;
3. Fédérer l'industrie française de la sécurité et en faire un champion international ;
4. Contribuer à l'héritage du programme olympique et développer un modèle exportable.

Accompagnant l'ensemble des phases du projet, ces livrables ont été **structurants** dans les phases d'architecture, d'analyse des besoins et d'orientation des plans d'expérimentation.

Expérimentations | L'ensemble de la filière, le ministère de l'Intérieur, l'ANSSI et le SGDSN se sont unis à travers des travaux communs : 192 expérimentations pour éclairer le savoir-faire français au profit des FSI

Le programme d'expérimentations est une véritable réussite de par son caractère **innovant** qui résulte de la collaboration entre le ministère et les entreprises et avec une réelle fédération des forces. Les **192 expérimentations** ont permis de **mettre en valeur les technologies françaises** auprès des forces de sécurité et de les **tester en conditions opérationnelles**, au plus près de leurs besoins. L'ensemble de la filière française est engagée dès lors dans l'objectif de **soutenir la modernisation des FSI** (Forces de Sécurité Intérieure), s'inscrivant ainsi dans une logique d'héritage.

La mobilisation de la filière française s'est particulièrement illustrée en 2022, dans le cadre de la mise en œuvre des expérimentations qui ont permis la valorisation de solutions issues d'industriels membres de l'ACN telles que : Anozr Way, Atos, Citalid, Egidium Technologies, Idemia, Orange, Owlint, Sahar, Thales, XXII, YesWeHack, Yogosha.

Le mode de sélection par appels à manifestation d'intérêt largement relayés a permis l'analyse de **687 solutions** issues de **171 sociétés** différentes.

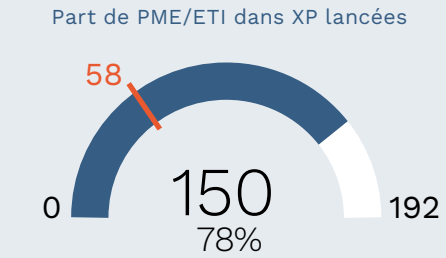
Brique	Nb Sociétés postulantes	Nb Solution analysées	Nb Sociétés participantes	Nb Solution Expérimentées
Moyens de commandement & Hypervision	59	195	30	52
Vidéoprotection	16	116	8	23
Cybersécurité	55	122	26	43
Bulle 3D - Très basse Altitude	17	117	5	20
Autres Domaines :				
Nautique	29	59	15	23
Gestion de foules & flux	17	29	12	17
NRBCE	17	49	10	14
GLOBAL	171	687	89	192

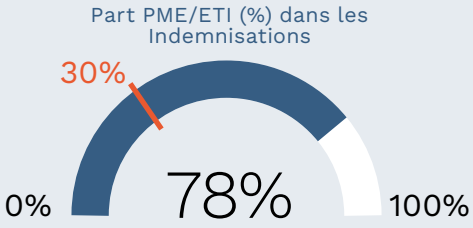
Les expérimentations ont permis de **dégager des axes essentiels de renfort technologique permettant ainsi d'améliorer l'efficience des forces**. La démarche mise en œuvre a permis de dégager des besoins communs et une action volontaire du ministère permettra de passer à l'étape suivante en proposant :

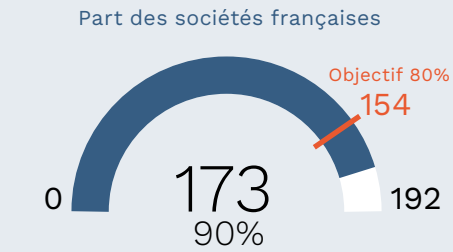
- Le regroupement d'achats communs ;
- La standardisation des technologies au profit de l'interopérabilité des forces ;
- L'utilisation de plateformes mutualisées.

Cette étape doit se matérialiser par des plans d'acquisitions sur chacune des briques des expérimentations, les deux principales étant la **cybersécurité** et les **centres de commandement** :

- **16 projets de cyber-sécurisations coconstruits avec le ministère de l'Intérieur** autour de **3 échéances** : la Coupe du monde de Rugby 2023, les Jeux Olympiques 2024 et la LOPMI échéance 2027.
- 3 axes de modernisation autour de la convergence des centres de commandement, de la structuration, de la collecte et de la restitution de leurs données.







Notre futur | Utiliser les travaux initiés comme un accélérateur de particules pour l'après-JOP2024

- **Capitaliser sur la démarche,** cristalliser les initiatives en cours, notamment en permettant les acquisitions de technologies pertinentes pour les FSI et faire du projet JO un accélérateur de particules pour l'ensemble de la filière et la modernisation du ministère.
- **Poursuivre la structuration** de la filière mobilisée autour d'une équipe de marque, d'actions de communication communes et de coordination avec les différents acteurs.
- **Mettre en œuvre une collaboration** permanente avec le ministère de l'Intérieur au travers d'une **interface dédiée.**
- **Lancer un programme d'export du savoir faire de la filière française** coordonné et piloté.

Soutenir la modernisation des forces de sécurité

Assurer la sécurité des jeux Olympiques de Paris 2024

Structurer et développer la filière des industries de sécurité via un événement majeur et mobilisateur

Bâtir l'héritage des jeux

LA SÉCURITÉ DES JOP2024 VUS DU MINISTÈRE DE L'INTÉRIEUR ET DE L'OUTRE-MER.

Olivier de Mazières

Délégué ministériel aux partenariats, aux stratégies et aux industries de sécurité (DPSIS)

Les Jeux olympiques et Paralympiques de Paris 2024 sont à ce jour le plus grand événement organisé en France, par son ampleur et sa durée. Assurer la sécurité d'un tel rendez-vous est un défi majeur. L'évolution des menaces, encore accentuée par l'usage massif du numérique, exige que le ministère de l'Intérieur et des outre-mer adapte en permanence sa réponse.

Cette dernière ne repose pas seulement sur les moyens mobilisés par les pouvoirs publics. Elle exige aussi l'intervention des femmes et des hommes qui font vivre le continuum de sécurité globale, ainsi que celle des entreprises capables d'apporter les ressources techniques nécessaires à la protection des personnes et des biens.

Cette mobilisation des acteurs et des technologies implique une juste mesure des besoins, une coordination des acteurs privés et publics et le respect d'un cadre juridique strict en matière de libertés.

Fin juillet 2021, la DPSIS s'est vue confier le pilotage d'un programme d'expérimentations technologiques de sécurité répondant à ces enjeux. Il répond à un engagement de l'Etat dans le contrat de filière des industries de sécurité, cosigné en janvier 2020 par le ministre de l'Intérieur.

Outre la sécurité des JO et grands événements, il visait à accélérer la transformation des forces et à renforcer les synergies avec les industriels fédérés dans le comité stratégique de filière (CSF-IS). Il s'agissait aussi de développer des outils technologiques interopérables entre les acteurs, adaptés à des menaces évolutives et testés en conditions réelles en vue d'éventuelles acquisitions.

Un budget de 21,5 M€. a été fléché sur le plan de relance 2022 pour organiser ces expérimentations et indemniser les industriels.

L'expression des besoins a mobilisé les forces, la CNSJ, les opérateurs de transports et plusieurs acteurs publics (SGDSN, DIJOP, DGTIM) autour de 7 priorités : centres de commandement, cybersécurité, traitement de l'image, sécurité très basse altitude (dont la lutte anti-drones), NRBC-E, sécurité nautique et gestion des flux.

Les 192 solutions testées (sur près de 700 proposées par les industriels) émanent pour 90 % de sociétés françaises et pour 77 % de start-ups, PME et ETI.
Les directions métiers ont déjà programmé des achats pour un montant évaluatif de plus de 60 M€. dont près de la moitié en 2023. D'autres acquisitions restent à chiffrer en matière notamment de centres de commandement, de cybersécurité, de protection des frontières et de vidéo intelligente, avec la mise en œuvre de l'expérimentation prévue par la récente loi relative aux Jeux Olympiques.

Ces derniers ont joué le rôle d'un accélérateur de particules pour le continuum de sécurité globale. Par-delà les achats, ces expérimentations ont aussi permis aux industriels de faire évoluer leurs produits pour toujours mieux répondre aux besoins des forces et à ces dernières de mesurer pleinement la disponibilité, la qualité et la densité des solutions souveraines.

Si cet héritage est dense, solide et pertinent, c'est d'abord parce qu'il est empirique, fondé sur des échanges permanents entre public et privé, concepteurs, intégrateurs et utilisateurs. Les essais en situation réelle ont permis de converger vers des solutions qui collent à la réalité des besoins et aux contraintes du terrain. C'est une méthode qui pave le chemin des coopérations futures et esquisse un modèle de sécurité éthique pour les grands évènements à venir, au bénéfice de la protection de nos concitoyens, de l'efficacité de nos forces et de la performance de nos entreprises.

La très prochaine création au sein du ministère de l'Intérieur et des Outre-mer d'une Direction des Entreprises et Partenariats de Sécurité et des Armes (DEPSA), ainsi que la mise en place d'un centre de R&D permettra de dynamiser cet effort et de resserrer ce lien capital entre les forces et les industriels de la sécurité.

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

5.2 Les tendances réglementaires

5.2.a. Paysage réglementaire européen : un marché unique du numérique de confiance à concrétiser

Au fur et à mesure que la transition numérique s'opère, les technologies développées sont devenues indispensables au quotidien de leurs utilisateurs. Ces nouveaux usages entrainent de nouveaux risques qu'il est nécessaire de maitriser. Pour répondre efficacement aux cyberattaques transfrontalières qui en découlent et protéger ses valeurs fondamentales, **l'Union européenne s'est dotée d'un programme ambitieux « Pour une Europe numérique » qui vise à positionner l'UE au cœur de cet enjeu majeur d'ici à 2030.** Ce programme qui se décline sous la forme de nombreuses initiatives réglementaires, adresse les objectifs de protection de l'UE face aux risques induits par le numérique (cybersécurité, cyber résilience, etc.) mais affiche également l'ambition de doter l'Europe d'une économie numérique de premier plan, en régulant le marché numérique, en stimulant la compétitivité des acteurs de l'écosystème ainsi que la recherche et l'innovation pour assurer la souveraineté technologique européenne.

La régulation du marché numérique

Dans un premier temps, l'Union européenne a souhaité **protéger le marché numérique européen des contenus** (pédopornographie, terrorisme, ...) et des produits illicites (contrefaisants, dangereux, ...) en ligne en harmonisant les législations nationales déjà applicables. Le *Digital Service Act* (DSA) s'appliquera en ce sens aux « très grandes plateformes » (plus de 45 millions d'utilisateurs actifs chaque mois, soit 10% de la population européenne) dès que la Commission les aura désignées, et dès le 17 février 2024 pour le reste des plateformes.

Dans un second temps, le *Digital Market Act* (DMA) protège le droit de la concurrence européen **des éventuelles pratiques déloyales des « contrôleurs d'accès »** (plateformes en ligne solide et pérenne à forte position fournissant un service de plateforme essentiel) entre en application le 2 mai 2023.

La protection des acteurs du marché numérique

L'Union européenne a souhaité **élever le niveau commun de cybersécurité** sur l'ensemble de son territoire **pour garantir un cyberespace de confiance et renforcer la coopération entre Etats membres.** Pour cela, elle a étendu le champ de la directive NIS avec de nouveaux secteurs essentiels et importants au maintien de l'économie et de la société afin de renforcer la cybersécurité de l'ensemble de la chaîne d'approvisionnement. La directive NIS 2 prendra effet dès octobre 2024.

L'ACN a publié début 2022 ses propositions pour la Présidence Française de l'Union Européenne.

Rapport ACN
«Présidence Française de l'Union Européenne : Propositions de l'ACN»
disponible en téléchargement sur
www.confiance-numerique.fr

Le renforcement de la résilience collective

L'Union a également entrepris de **limiter les risques** posés par **la profonde transformation numérique des services financiers et l'interconnexion croissante des réseaux et infrastructures critiques.** Le règlement DORA sur la résilience opérationnelle numérique du secteur financier publié le 16 janvier 2023, entrera en vigueur dès le 17 janvier 2025 harmonisera la gestion des risques dans ce secteur.

Ensuite, le projet de *Cyber Resilience Act* (CRA), encore en discussion, **établira des exigences communes de cybersécurité pour tous les produits électroniques et numériques mis sur le marché interne européen.**

L'Union souhaite désormais renforcer **la solidarité cyber et les capacités de gestion en cas de crise** à travers le *Cyber Solidarity Act* annoncé le 18 avril 2023, financé à hauteur d'1,1 milliards d'euros et qui sera composé de trois piliers : un **Bouclier Cyber européen** (réseau de SOC-*Security Operations Centers* nationaux et transfrontaliers, un **Mécanisme d'Urgence Cyber** (avec notamment la création d'une Réserve Cyber européenne) et **un Mécanisme d'Analyse des Incidents de cybersécurité.** Ce dispositif sera accompagné d'un renforcement des compétences en la matière afin de remédier à la **pénurie de talents** dans la cybersécurité avec la création d'une *Cyber Skills Academy.*

Enfin, l'identité numérique et l'identification/ authentification sécurisée des européens est également au cœur des évolutions réglementaires avec la révision, en cours du règlement eIDAS. La réglementation eIDAS-2 fixe le cadre européen relatif à une identité numérique (identification électronique). Le règlement révisé vise **à assurer l'accès universel des personnes et des entreprises à une identification et une authentification électroniques sécurisées et fiables au moyen d'un portefeuille numérique personnel.**

La proposition imposera aux États membres de délivrer un portefeuille numérique dans le cadre d'un schéma d'identification électronique notifié, basé sur des normes techniques communes (*Architecture and Reference Framework* – ARF) et après une évaluation de conformité obligatoire.

Focus - Point de vue de la presse

UN EXCÈS DE RÈGLES PEUT NUIRE À LA CONFIANCE

Delphine Sabattier

Delphine Sabattier est journaliste présentatrice et productrice, spécialiste en France des sujets d'innovation et de politiques numériques.
Elle explore et vulgarise les enjeux de transformation de la société et des écosystèmes à travers des articles de presse, ses éditoriaux TV sur LCP, des productions audiovisuelles, et son émission quotidienne de découverte et de réflexion sur l'innovation, Smart Tech sur la chaîne B SMART TV (https://www.bsmart.fr/emissions/smart-tech). Auparavant, Delphine a dirigé les plus prestigieux médias d'information dédiés aux nouvelles technologies (Science & Vie micro, 01net...). Elle est aujourd'hui une figure incontournable de l'information tech.

« J'étais là avec mon micro, prête à cueillir le Commissaire européen Thierry Breton pour une déclaration, une réponse aux attentes sur la sécurisation de l'espace numérique : j'ai été servie ! Le discours surprise qu'il a délivré devant les professionnels de la cybersécurité réunis au FIC2023 à Lille début avril avait tout pour plaire à son public : « La résilience cyber ne peut devenir qu'un sujet européen », « nous coordonner est indispensable » a-t-il martelé, déroulant la nouvelle doctrine de Défense de l'Europe et dévoilant le projet de bouclier cyber européen.

Ce « dôme », explique le Commissaire Breton, repose sur quatre piliers : protéger, détecter, défendre et dissuader. Pour cela, nous avons besoin de technologies de pointe, d'infrastructures, de coopération... et de sanctions. La Commission européenne s'emploie ainsi avec vigueur à établir les nouveaux cadres à respecter. Une règlementation très attendue pour créer les conditions de la confiance, mais qui pourrait paradoxalement jouer contre notre écosystème.

En effet, ignorer les impacts de la règlementation sur nos acteurs européens serait une erreur. Cela reviendrait à pénaliser notre industrie, affaiblir nos forces et par-là même nous éloigner encore un peu plus de la quête de souveraineté. Or, la maîtrise des technologies et des données est une essentielle à la confiance. Certes, tout le monde s'accorde intellectuellement sur ce point. La « souveraineté numérique et industrielle » est de tous les discours politiques. Mais dans les faits ?

A chaque nouvelle règle, c'est l'annonce d'un nouvel exercice acrobatique de mise en conformité... où les premières sous pression sont les entreprises européennes du secteur. L'Europe est leur marché natif. Les sanctions leur sont applicables de fait... là où les mises en demeure des big tech sont bien plus complexes et longues à arriver. Quant au risque encouru : l'amende pour une société européenne est souvent plus difficile à encaisser.

Dommage collatéral, à ne pas négliger

Vous vous souvenez du témoignage d'Olivier Magnan-Saurin, de Fidzup ? Le 5 février 2020, il écrit, rageur, « La CNIL nous a tuer ». Son entreprise française n'a pas survécu à la mise en application du RGDP. Il reconnaît les progrès nécessaires apportés par le règlement sur la protection des données personnelles, mais s'interroge : « Comment créer des champions européens dans ce contexte si l'application de nos lois est plus contraignante pour les sociétés du vieux continent que pour le reste du monde ? Comment reprendre le leadership dans le domaine de la technologie ou du stockage des données si nous renforçons les positions des Américains ou des Chinois ? ».

Ces inquiétudes restent d'actualité chez les dirigeants que je reçois dans Smart Tech, avec l'arrivée du Cyber resilience act ou encore le Secnumcloud français. Or, la confiance passe par la capacité de l'Europe à développer ses propres technologies sur le marché intérieur. Aujourd'hui, les menaces cyber « d'ampleur », ce sont des menaces géopolitiques. C'est pourquoi l'Union européenne doit se donner les moyens de devenir une puissance technologique dans la cyber : soutenir, consolider, renforcer son écosystème pour protéger sa souveraineté.

Et si l'on commençait à se faire confiance ?

Mon point de vue : pour développer la confiance, oui il faut des règles protectrices, contraignantes, appliquées à tous… mais il faut aussi que l'Europe apprenne à se faire confiance.

Apprendre à se faire confiance notamment entre États membres, et c'est le sens du Cyber solidarity act qui est sans doute le texte le plus conciliant que la Commission publiera dans le registre de la cybersécurité.

Mais l'Europe doit aussi croire en la capacité de ses acteurs technologiques à devenir des puissances. Des pépites de la cybersécurité et plus largement de la tech, nous en avons ! J'en reçois régulièrement en plateau. Dommage, elles captent plus facilement des marchés internationaux que les carnets de commande de l'Etat français ! Elles défendent un Small Business Act à l'européenne… et aimeraient que la Commission, lorsqu'elle rédige ses règlements, n'oublie pas de considérer les impacts sur son propre écosystème.

Je m'en fais l'écho ici avec la conviction que pour faire bloc face aux grandes menaces, on devrait commencer à se faire confiance en Europe. N'étouffons pas nos forces d'innovation internes. Sinon, qui tiendra nos boucliers ?

Edouard Jeanson, Vice-Président de l'ACN, interviewé par Delphine Sabattier dans SMART TECH sur la création d'un « marché unique du numérique ». Émission diffusée en direct sur B Smart, le 21 février 2022.

5.2.b. Les initiatives nationales de cybersécurité

Afin de répondre au défi de la souveraineté numérique, de l'autonomie stratégique et de l'amélioration de la résilience du pays, le Président de la République française a annoncé, en février 2021, **le déploiement d'une Stratégie Nationale pour la cybersécurité.** Les objectifs fixés sont de tripler le chiffre d'affaires de la filière, doubler le nombre d'emplois et faire émerger au moins 3 licornes d'ici 2025. Diverses actions ont été lancées en ce sens **dont les parcours de l'ANSSI** destinés à élever le niveau de cybersécurité en France et faisant partie du volet cybersécurité du plan France Relance. L'enjeu désormais est d'augmenter fortement la résilience de tous les acteurs publics et privés sur l'ensemble du territoire et notamment d'approfondir la protection des organisations les plus vulnérables, à savoir les établissements de santé, ainsi que les PME et les ETI.

Plusieurs initiatives ont d'ores et déjà été initiées en ce sens par le ministre délégué chargé de la Transition numérique et des Télécommunications, Jean-Nöel Barrot, le ministre de l'Intérieur et de l'Outre-mer, Gérald Darmanin et le ministre de la Santé et de la Prévention, François Braun **afin de renforcer la cybersécurité des établissements de santé,** particulièrement ciblés par les cyberattaques au cours de ces deux dernières années.

Concernant la protection des PME et les ETI, l'Etat a également entrepris de mettre en place un bouclier cyber, avec un financement de 25 millions d'euros afin de les accompagner dans leur démarche de cybersécurisation. Ce bouclier sera composé de 3 volets : sensibilisation, mise à disposition d'un autodiagnostic cyber et un dispositif de sécurisation.

Enfin, la France s'est dotée d'un **Cyberscore**, qui doit entrer en vigueur en octobre 2023, et qui prend la forme d'un **affichage du niveau de protection offert par les grandes plateformes numériques,** destiné au grand public, tant du point de vue de la cybersécurité, que de la protection des données personnelles mais aussi de l'exposition à l'application extraterritoriale de lois étrangères. Une consultation publique a été lancée par la Direction Générale des Entreprises (DGE) afin de finaliser ce projet, et l'ACN y a répondu pour porter les messages de la filière sur ce projet de Cyberscore et sa mise en œuvre concrète.

Par ailleurs, **les comités stratégiques de filières, et principalement le CSF « Industries de Sécurité », poursuivent leurs travaux** en complément de ces initiatives publiques. La feuille de route du CSF Industries de Sécurité est en cours de mise à jour pour parvenir à l'été 2023 à la signature d'un contrat de filière qui comprendra des travaux sur notamment les chantiers prioritaires suivants : Sécurité des frontières, Opérations de sécurité au quotidien, Sécurité du système de santé, Cyber des PME, certification / réglementation, Sécurité des collectivités, Identité numérique, Promotion, Stratégie, Sécurité des JO 2024, Attractivité et compétences et Transition écologique.

5.2.c. Définir les critères de l'Intelligence Artificielle de Confiance

L'intelligence artificielle, au sens de la proposition d'*AI Act* de la Commission européenne se définit comme « un logiciel qui est développé au moyen d'une ou plusieurs des techniques et approches [...] et qui peut, pour un ensemble donné d'objectifs définis par l'homme, générer des résultats tels que des contenus, des prédictions, des recommandations ou des décisions influençant les environnements avec lesquels il interagit ».

L'IA occupe une place de plus en plus prégnante dans le quotidien de ses utilisateurs. Souvent mise en avant dans la seule logique de marketing, cette technologie demeure **assez largement méconnue et fait l'objet d'une large mésinformation** voire désinformation suscitant des craintes et de nombreux débats qui contribuent à freiner son développement.

Les entreprises de la filière de la Confiance Numérique considèrent que l'IA constitue une brique technologique essentielle pour notre avenir numérique, mais aussi que **sa maîtrise est un enjeu majeur pour la souveraineté numérique et l'autonomie stratégique de notre pays.**

Pour autant, le débat public doit avoir lieu sur l'ensemble des questions que peuvent soulever l'IA et ses différents usages. Mais ce débat doit être éclairé et se fonder sur la réalité technique de l'IA dont il revient au législateur de fixer le cadre à l'intérieur duquel ces solutions pourront être développées en toute confiance et dans le respect de l'ensemble des valeurs fondamentales qui sont celles de nos sociétés françaises et européennes.

C'est pourquoi l'ACN s'est doté d'une feuille de route consistant à définir les critères (juridiques, techniques et éthiques) objectifs qui pourraient servir de références pour parvenir à définir avec précision et clarté ce qu'est une IA de confiance. C'est notamment l'objet d'un livre blanc en cours de rédaction au sein de son groupe de travail dédié à l'Intelligence Artificielle de Confiance. Ce livre blanc se proposera de présenter les différentes facettes et les différents usages de cette technologie créatrice de valeur ajoutée afin de dépassionner et d'éclairer le débat public et de proposer des critères pour distinguer les IA de confiance.

Ce livre blanc aborde en premier lieu **le cadre juridique de l'IA et ses limites.** L'IA est considérée par les textes actuellement en vigueur comme une « nouvelle technologie » qu'il convient de contrôler par des obligations contraignantes édictées pour dans un cadre plus global et non spécifique à l'IA.

S'en suivent de **nombreuses interprétations par nature inadaptées** qui ne sont pas satisfaisantes dans la mesure où elles conduisent à freiner le développement, en France et en Europe, de ces technologies essentielles à notre maîtrise du monde numérique dans le futur. Pour y remédier, **il est désormais urgent que des réglementations spécifiques à l'IA soient conçues, adaptées aux usages nombreux et divers de cette technologie**, afin de permettre aux acteurs de ce domaine de pouvoir développer ces technologies dans un cadre adapté. **La proposition d'*AI Act* de la Commission européenne est en ce sens bienvenue.** Le nouveau cadre de l'IA doit permettre à un écosystème de confiance de gagner en compétitivité et de favoriser les synergies dans la filière. Ce cadre en construction semble être une base solide à la création d'une norme internationale d'IA de Confiance.

Au-delà, la confiance s'établit également dans le domaine technique. Des notions telles que l'explicabilité, la prédictibilité, la transparence, la limitation des biais, la qualité des bases d'apprentissage doivent trouver **des déclinaisons techniques précises, vérifiables et auditables.**

Enfin, la confiance s'établit par **l'acceptabilité sociale et l'éthique de l'IA.** Elle doit être développée conformément aux valeurs fondamentales de l'Union européenne et à des principes prédéfinis comme ceux de la Charte éthique européenne d'utilisation de l'IA dans les systèmes judiciaires et leur environnement adoptée les 3-4 décembre 2018. L'ACN choisit de concentrer son attention sur **les principes de primauté de l'Homme** afin qu'il soit toujours au cœur de cette technologie et qu'elle ne décide pas isolément d'un contrôle humain, la nécessité de performance afin de s'assurer qu'elle soit adaptée, nécessaire et proportionnée et que cette technologie soit environnementalement acceptable. Ces principes doivent néanmoins être partagés, le plus largement possible, dans le débat public afin de **créer un consensus autour de cette notion de confiance, indispensable au développement serein de technologies stratégiques pour notre avenir.**

Focus ANSSI - Volet cybersécurité du plan France Relance

Bilan des actions menées

Dans le cadre de France Relance, un « volet cybersécurité » a été mis en place, sous pilotage de l'Agence nationale de la sécurité des systèmes d'information (ANSSI). Ce plan, qui s'élevait à 176 millions d'euros sur 2021-2022 a permis de déployer plusieurs dispositifs notamment **au profit des collectivités territoriales, des établissements de santé et pour la sécurité des systèmes et réseaux de l'Etat.**

Une stratégie gagnant / gagnant au coeur des actions :
Augmenter la cybersécurité de l'Etat et des services publics, via l'acquisitation de prestations et produits pour renforcer l'offre européenne

Le bilan global de ce plan est extrêmement positif : il a permis une augmentation concrète du niveau de cybersécurité des bénéficiaires et un large déploiement de nombreuses solutions, très majoritairement européennes. La mobilisation de l'écosystème des prestataires et éditeurs de solutions pour répondre aux besoins des utilisateurs, exprimés au travers des dispositifs proposés, a notamment permis cette réussite.

Actions réalisées

Les dispositifs ont privilégié le subventionnement des bénéficiaires concernés, avec un co-financement nécessaire. Ce mécanisme offre l'avantage d'impliquer et de responsabiliser chacun dans ses projets de cybersécurité, pour les aider à identifier et mettre en œuvre les moyens humains, financiers, administratifs et techniques nécessaires.

Un ensemble de 4 grands chantiers, tous menés à leur terme

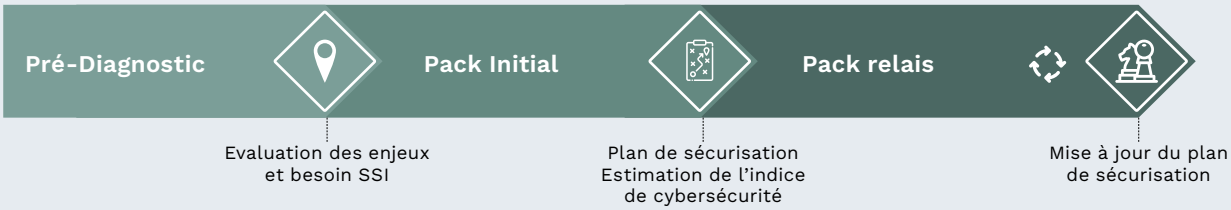
100 M€ — Parcours de cybersécurité
- Diagnostic
- Sécurisation
- Sensibilisation
- Accompagnement

Appels à projet — 27 M€
Soutien Financier à des projets cohérents de cybersécurité

17 M€ — CSIRT régionaux et sectoriels
Développement d'un réseau de centres de réponse à incident

Produits et services mutualisés de cybersécurité — 32 M€
Services et produits cyber pour les agents de l'Etat
Capacités accrues de détection

Les parcours de cybersécurité ont permis d'accompagner 950 bénéficiaires au travers d'une démarche formalisée grâce à des concepts et guides préalablement produits par l'ANSSI : guide d'hygiène ou guide sur les attaques par rançongiciels, mais aussi avec l'appui des experts de l'agence qui ont participé à la phase de cadrage et à la définition des Parcours. La conception par les experts de l'ANSSI assure ainsi la pertinence technique du dispositif. Les retours d'expérience opérationnels ont été pris en compte pour l'adapter au plus près des besoins. Plus de 170 prestataires terrain sont aujourd'hui impliqués dans ces parcours pour aider les bénéficiaires.



L'investissement réalisé par les bénéficiaires, au travers du cofinancement des projets retenus, est en moyenne plus de 20% supérieur à l'attendu, montrant à la fois le fort besoin et la prise de conscience des enjeux. La mobilisation de ces moyens sur le long terme, au travers d'un budget cyber augmenté et de moyens humains dédiés, doit permettre de pérenniser les actions que l'ANSSI a permis d'initier. Notons que plus de 95% des solutions de sécurité acquises dans le cadre des parcours de cybersécurité sont européennes.

La montée en puissance d'un réseau de CSIRT régionaux

La création dans chaque région d'un centre de réponse à incident cyber est une solution pertinente pour soutenir les victimes, du secteur privé comme public, de taille intermédiaire, face à la multiplication des attaques cyber. Il s'agit de limiter les impacts économiques et sociaux des cyberattaques en accompagnant leur résolution rapide. Ces centres doivent devenir de véritables services de réponse à incident d'intérêt général, adapté aux besoins des PME, ETI, et structures publiques, permettant le suivi des incidents et la mise en relation des victimes avec les prestataires adaptés pour les accompagner.

Au travers du plan de relance, 12 régions métropolitaines sur 13 ont exprimé leur engagement et ont été soutenues financièrement, par un subventionnement d'un million d'euros, et techniquement, par le suivi d'un programme d'incubation pour une mise en route accélérée. 7 CSIRT sont d'ores et déjà opérationnels, tous devraient l'être d'ici la fin de l'année 2023.

Côté outre-mer, ces structures sont plutôt orientées vers le développement de l'écosystème local, pour faire émerger l'offre de solutions et de services tout en sensibilisant sur la menace pour développer la demande. Un tel « centre de ressources cyber » est soutenu pour le côté Atlantique (CRC Caraïbes), un autre est soutenu pour la partie Océan Indien (CRC Réunion), et un dernier est soutenu pour le côté océan Pacifique (CRC Nouvelle-Zélande).

Ces centres vont permettre, dans chaque territoire, la concentration des informations sur les attaques subies par ces structures de taille intermédiaire. Ils doivent devenir les interlocuteurs des victimes pour leur mise en relation avec les prestataires de réponse.

En savoir plus :
Le volet cybersécurité de France Relance
Les CSIRTs régionaux

VI. LES TENDANCES TECHNOLOGIQUES

L'innovation technologique est le principal moteur de la croissance de la Confiance Numérique française et mondiale depuis plus de 10 ans et cette tendance devrait se poursuivre à minima durant les 10 prochaines années. Les développements technologiques affectent la Confiance Numérique de manières différentes et complémentaires.

6.1 Les innovations électroniques et numériques qui génèrent de nouveaux marchés

Les innovations issues des industries électroniques et numériques impactent presque tous les secteurs des économies modernes et génèrent de ce fait de nouveaux marchés pour la Confiance Numérique.

■ **Les systèmes et composants électroniques sont marqués par la miniaturisation couplée à la baisse des coûts.** Cette tendance, incarnée par la Loi de Moore, a marqué très fortement l'économie mondiale ces 50 dernières années et devrait se poursuivre à minima sur la décennie à venir avec le développement des mémoires 3D multicouches et la miniaturisation des processeurs. Cependant, cette tendance touche à sa fin. Les investissements pour continuer la Loi de Moore et se maintenir dans la course à l'innovation croissent de façon exponentielle et atteignent déjà des niveaux tels que seulement sept entreprises se maintiennent au niveau mondial : Samsung (Corée du Sud), TSMC (Taïwan) et Intel (États-Unis) dans les processeurs et Samsung (Corée du Sud), SK Hynix (Corée du Sud), Micron (États-Unis), Western Digital (Etats-Unis) et Toshiba (Japon) dans les mémoires.

En conséquence de la miniaturisation et de la baisse des coûts, les produits électroniques se démocratisent, y compris en matière de Confiance Numérique : capteurs, système de traçage et localisation, ainsi que tous les sous-systèmes inclus dans les segments électroniques de la filière. Il s'agit d'un phénomène de long terme. A court terme, la croissance des composants électroniques est cyclique et la période 2020-2022 a, au contraire, vu les prix des semi-conducteurs s'envoler. Depuis le début de l'année 2023, la baisse des prix de semi-conducteurs a repris son cours.

Dans les cinq années à venir, seules les augmentations des prix de l'énergie sont à même de contrebalancer la baisse des prix associée à la poursuite de la miniaturisation de l'électronique, en fonction de l'amplitude qu'elles vont avoir, en particulier en Europe.

■ **La transformation digitale,** c'est-à-dire la numérisation des outils, produits et services dans tous les secteurs de l'économie. Ce processus de digitalisation en est encore à son commencement à l'échelle mondiale. Il conduit à une croissance toujours plus importante de la part qu'occupent les enjeux numériques et cette tendance devrait durer pour à minima les 20 années à venir au travers du déploiement du **continuum *Cloud-to-Edge*** et ses débouchés en matière d'IoT industriels (logiciel embarqué, connectivité, *cloud*).

Le croisement de ces deux tendances génère de nombreux marchés émergents et porteurs pour la Confiance Numérique.

1. Sécurité des objets connectés. À terme, si chaque objet devient connecté, chaque objet nécessitera un outil cyber pour le sécuriser. En outre, l'interconnexion des objets connectés décuple les risques en matière de cybersécurité en rendant vulnérable des réseaux entiers. En conséquence, l'interconnexion des objets entre eux représente un potentiel de croissance gigantesque pour les produits et les services de cybersécurité associés : identification et authentification des IoT, éléments sécurisés, sécurité des communications (5G / 6G, protocoles de communication IoT longue distance type LoRa et Sigfox ou bien courte portée type Wi-Fi, *Z-Wave*, *Bluetooth Low Energy*...), des infrastructures, des applications (hyperviseurs, etc.)... Jusqu'à présent, la croissance issue des objets connectés a été encore faiblement ressentie par les acteurs de la filière française de sécurité, bien que nombre d'entre eux aient déjà travaillé à une offre dédiée depuis plusieurs années. Les progrès dans la standardisation et l'interopérabilité des architectures IoT sont à même d'accélérer la croissance future.

■ **Automobile connectée.** Le principal segment déjà en forte croissance est celui de la sécurisation des automobiles et de leurs communications : *Vehicle-to-Vehicle* (V2V), *Vehicle-to-Infrastructure* (V2I : péage, etc.), *Vehicle-to-Device* (V2D : *Smartphone*, etc.).

■ ***Smart & Safe City.*** Le développement des objets connectés dans les villes à des fins de sécurité est le deuxième segment qui a généré la croissance la plus importante au niveau mondial chez les acteurs de la sécurité numérique et de la cybersécurité en lien avec les objets connectés depuis 2015. Les acteurs qui ont le plus bénéficié de la thématique *Safe City* sont les grands intégrateurs (Thales, Accenture, Capgemini, etc.). La *Safe City* est globalement moins porteuse en France qu'à l'étranger (que ce soit en Chine, aux États-Unis ou dans de nombreux pays émergents) pour trois raisons principales : l'administration française qui s'est construite autour de processus non digitaux, la grande diversité des acteurs publics en France (état central, régions, départements, communes, communauté de communes, etc.), et l'austérité budgétaire.

■ **Sécurisation de l'Industrie 4.0.** La croissance associée au déploiement et à la sécurisation de l'Industrie 4.0 devrait se faire de plus en plus ressentir sur les années à venir. Cependant, installer des objets connectés à l'intérieur d'une usine ne nécessite pas forcément le développement de solutions dédiées aux objets connectés de la part des fournisseurs cyber car les objets peuvent être tous reliés au serveur central de l'usine. Autrement dit, la technologie IT-OT classique et un peu plus ancienne est suffisante. En conséquence, le développement des objets connectés à minima dans l'usine 4.0 ne se traduit pas par une augmentation significative des commandes concernant la mise en place de solution spécifiques de sécurisation d'objets connectés dans ces usines.

La France dispose d'acteurs importants sur l'ensemble des segments de sécurité associés à la sécurisation des IoTs, mais manque d'acteurs nationaux de taille significative pour le déploiement des plates-formes de services associés aux objets connectés (du type des GAFAMI aux États-Unis ou des BATX en Chine).

2. Souveraineté de la donnée et *clouds* souverains. En parallèle du foisonnement technologique en matière d'électronique autour du stockage et du traitement des données (mémoires non-volatiles 3D multicouches, puces neuromorphiques, calcul quantique, calcul photonique, photonique intégrée, réseaux d'interconnexion photonique, calcul de haute performance (HPC), etc.), le nombre et le volume des bases de données croît de manière exponentielle (*big data*). La problématique de sécurisation de ces jeux de données prend de plus en plus d'importance, que ce soit pour des raisons régaliennes (services publiques, bases de données critiques), économiques (protection des données sensibles des entreprises), ou citoyennes (droits du citoyen, protection des données personnelles, droit à l'oubli…).

A cet égard, **on assiste à la construction de plusieurs offres de *clouds* souverains de la part de l'écosystème français,** à l'image de l'offre « Numspot » portée par Docaposte et impliquant Dassault Systèmes, Bouygues Telecom et la Banque des Territoires. **A noter également la construction de la première plateforme *cloud* collaborative souveraine française** de la part des trois entreprises Olvid, Oodrive et Tixeo. D'autres offres de *cloud* de confiance ont été construites en France mais en partenariat avec les GAFAM, dans une logique de *cloud* de confiance : S3NS (Thales et Google), Bleu (Orange, Cap Gemini et Microsoft), ainsi q'une offre conjointe entre AWS et Atos.

3. Identités numériques. Fortement corrélée à la thématique de souveraineté de la donnée, la nécessité de la re-définition des identités numériques provient également du développement des outils électroniques et de la transformation numérique (« citoyenneté à distance »). La norme actuelle en France demeure l'existence simultanée de nombreuses identités décorrélées, avec un niveau de sécurité élevé (CNI, passeport), substantiel (identité numérique La poste, PVID) et faible (identités numériques délivrées très majoritairement par les acteurs du numérique américains du type GAFA pour le e-commerce), sans garantie de protection des données. L'alternative est le déploiement d'une identité forte et souveraine pour des applications régaliennes et associée à l'utilisateur qui gère ensuite comme il le souhaite ses autres identités qu'il dérive de la première. **La filière industrielle française dispose de tous les acteurs et de toutes les compétences nécessaires à cette alternative** (éléments sécurisés, *Identity & Access Management* (IAM), intégration des solutions, cryptographie, biométrie, PVID, etc.). Le projet prend forme depuis 2022 au niveau français autour **du déploiement de la Carte Nationale d'Identité Electronique (CNIe) et de FranceConnect, et au niveau européen autour du projet de portefeuille (*wallet*) d'identités numériques (eIDAS2).**

Une possibilité à l'avenir serait la synergie entre la thématique de l'identité numérique et celle de la souveraineté des données, avec le déploiement en Europe d'une identité numérique forte, certifiée par une organisation publique de confiance et associée à des identités dérivées centrées sur l'utilisateur ainsi qu'aux données de connexion, elles-mêmes stockées en Europe, et dont l'exploitation serait réservée sous condition à des acteurs uniquement européens.

4. La transformation digitale en particulier est le moteur de **la plupart des segments de la cybersécurité** : sécurisation des *clouds* d'entreprises, du télétravail, logiciels de renseignement et collecte d'information qui bénéficient de larges bases de données générées par le numérique, etc.

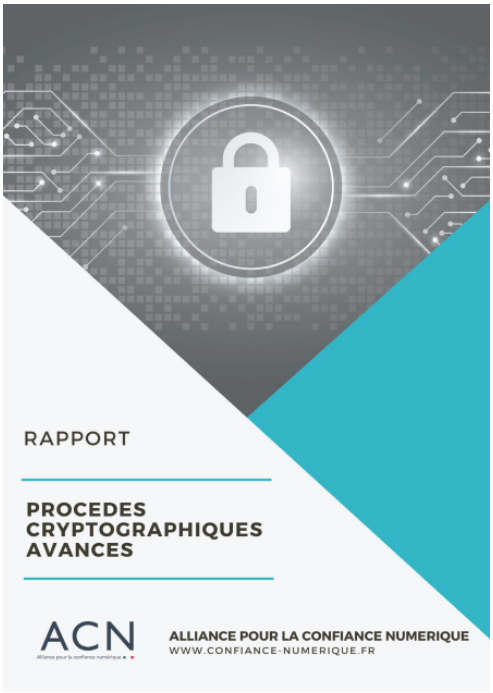
6.2 Les innovations propres à la filière qui génèrent de nouveaux produits

En parallèle -et étant donné que la Confiance Numérique est elle-même constituée intégralement de solutions électroniques et numériques- **les innovations issues de la Confiance Numérique** en elle-même génèrent de **nouveaux produits**, de nouvelles applications et donc de la croissance.

1. Cryptographie. La cryptographie regroupe l'ensemble des procédés visant par exemple à chiffrer des informations pour en assurer la confidentialité entre l'émetteur et le destinataire. Les développements technologiques en matière de cryptographie sont très nombreux et l'industrie française comme son écosystème de formation et de recherche se situent au meilleur niveau mondial dans ce domaine. Outre des champs technologiques déjà assez largement matures (cryptographie à clef publique...), les principaux champs d'innovations sont les suivants :

■ **Cryptographie légère (*Lightweight cryptography*).** Le développement rapide de l'IoT a un impact énorme sur tous les aspects liés à la cybersécurité. De récentes attaques massives contre des configurations IoT ont montré que de solides techniques cryptographiques doivent être utilisées pour assurer une sécurité globale du système. Malheureusement, dans le cas de l'IoT, où le coût est un paramètre important, l'utilisation de la cryptographie peut être limitée par la taille, la puissance et les performances informatiques locales des objets. Cela a donné naissance à un domaine de recherche très actif autour de la cryptographie dite légère. En bref, la cryptographie légère recherche de nouveaux algorithmes ou protocoles cryptographiques adaptés à la mise en oeuvre dans des environnements restreints, y compris les étiquettes RFID, les capteurs, les appareils de santé et de soins. La cryptographie légère sera progressivement utilisée dans tous les domaines IoT où le concept SWAP (taille, poids et puissance) tend à devenir critique. Les premières applications industrielles sont en train d'être développées et mises en place.

■ **Cryptographie post-quantique.** Les communications, terrestres ou satellitaires, tiennent une place centrale dans notre société et des outils efficaces ont été mis au point ces dernières décennies afin de sécuriser les données échangées et de se prémunir contre les attaques. Cependant, l'ordinateur quantique et sa puissance de calcul potentielle constitue une menace pour les données chiffrées avec ces méthodes qu'il pourrait décrypter en un temps record. Pour répondre à cette menace, la cryptographie post-quantique se base sur de nouveaux concepts mathématiques afin de chiffrer les messages et donc sécuriser le transport de l'information.



L'ACN a publié en mai 2021 un rapport sur les procédés cryptographiques avancés, dans lequel est décrit l'état de l'art pour chacune de ces technologies.

Rapport ACN
«Procédés cryptographiques avancés»
disponible en téléchargement sur
www.confiance-numerique.fr

■ **Chiffrement homomorphique.** L'énorme développement du *cloud computing* a généré un champ de recherche très actif autour du chiffrement dit fonctionnel et du chiffrement homomorphique : le chiffrement fonctionnel est un nouveau paradigme pour le chiffrement à clé publique qui permet à la fois un contrôle d'accès à granularité fine et un calcul sélectif sur les données chiffrées. Dans sa version la plus complète, le chiffrement entièrement homomorphe (FHE) permet le calcul sur des données chiffrées sans divulguer aucune information sur les données sous-jacentes. En bref, une partie peut chiffrer certaines données d'entrée, tandis qu'une autre partie, qui n'a pas accès à la clé de déchiffrement, peut effectuer aveuglément des calculs sur cette entrée chiffrée. Le résultat final est également chiffré, et il ne peut être récupéré que par la partie qui possède la clé secrète. Ce champ est très prometteur et les premières applications industrielles émergent.

■ **Cryptographie utilisant l'ADN.** Il s'agit d'une nouvelle branche de la cryptographie. Elle utilise l'ADN comme vecteur d'information et de calcul à l'aide de techniques moléculaires. Il s'agit d'un domaine relativement nouveau qui a émergé suite aux découvertes sur la grande capacité de stockage de l'ADN - qui est l'outil de calcul de base de ce domaine. Un gramme d'ADN stocke environ 108 To de données, ce qui dépasse la capacité de stockage de tout support de stockage électrique, optique ou magnétique. Les premières applications industrielles devraient émerger dans les prochaines années.

■ **Cryptographie utilisant des réseaux de neurones antagonistes génératifs (*GAN cryptography*).** Les réseaux de neurones antagonistes génératifs sont une innovation récente en matière d'intelligence artificielle. L'utilisation de ces algorithmes en cryptographie permet d'améliorer la qualité de certains systèmes. Ce domaine demeure pour le moment au stade de développement et les premières applications industrielles devraient émerger dans les prochaines années.

2. Eléments sécurisés (*Secure elements*). Ce domaine innovant est particulièrement important pour la France car toutes les technologies sous-jacentes y sont nées, permettant le développement de trois leaders mondiaux depuis la France : Thales, Idemia et STMicroelectronics. Les éléments sécurisés sont des composants micro ou nanoélectroniques comprenant une combinaison de logiciels embarqués sécurisés (SW) et de matériel (HW) et visant à être intégrés dans des dispositifs communicants afin de gérer de manière sécurisée toutes les interactions entre ces derniers et le monde extérieur en stockant des applications dédiées et des données confidentielles de manière chiffrée (cartes SIM, puces de cartes bancaires...).

Dans le contexte du développement des IoT, le segment des éléments sécurisés est marqué par le remplacement des cartes SIM (*Universal integrated circuit card*), par des éléments sécurisés miniaturisés et directement embarqués ou intégrés dans les systèmes auxquels ils se rattachent, voire sans aucune composante *hardware* (*soft secure elements*, *Trusted Execution Environment*). Le déploiement des éléments sécurisés embarqués (e-UICC) et des *Soft secure elements* a commencé et le déploiement massif des éléments sécurisés intégrés (i-UICC) ne devrait pas avoir lieu avant 2024, c'est-à-dire une fois que les problèmes d'assurance et de normalisation auront été résolus. La France domine actuellement ce secteur au niveau mondial avec l'Allemagne et devant la Chine, les Etats-Unis et la Corée du Sud. Les principaux concurrents des acteurs français au niveau mondial sont le néerlandais NXP, les allemands Infineon et Gieseke & Devrient, le sud-coréen Samsung et les chinois Shanghai Huahong et Shanghai Fudan Microelectronics. Il existe une menace potentielle à moyen terme pour les acteurs français en raison du manque de compétences en Europe et en France sur les technologies *More Moore* qui est susceptible de conduire les fabricants américains et asiatiques à acquérir des positions dominantes sur le segment des i-UICC. Les *Soft secure elements* représentent également une menace forte pour les acteurs français, principalement à travers les GAFAM américains et les BATX chinois qui peuvent tirer parti de leur position dominante pour imposer leurs solutions.

3. Intelligence Artificielle (IA). L'intelligence artificielle regroupe le développement d'algorithmes de *machine learning* (Réseaux de neurones artificiels, multicouches ou non, supervisés ou non, réseaux antagonistes génératifs…), et la problématique de l'*edge AI*, c'est-à-dire du design de puces et systèmes embarqués dédiés à l'exploitation d'algorithmes de *machine learning* (très gourmands en capacité de calcul et mémoire). Les développements en matière d'intelligence artificielle ne sont pas propres à la filière de sécurité mais de nombreuses adaptations et applications émergent sur la plupart des segments :

■ **Biométrie comportementale.** Les segments de l'identification et authentification des personnes, du contrôle d'accès et de la détection d'intrusion et alarme sont positivement impactés par le développement des solutions de biométrie comportementale : reconnaissance faciale, reconnaissance de signature, identification des personnes par une séquence d'images permettant de spécifier un comportement, etc. ;

■ **Agrégation et analyse des données collectées dans les segments de l'observation locale, de l'observation large zone et du renseignement et collecte d'information ;**

■ **Audit de cybersécurité.** En matière d'intelligence artificielle, la France bénéfice d'une excellence en matière de formation et de recherche et les acteurs français de la sécurité prennent d'assez fortes positions en matière d'applications de sécurité (notamment Thales Digital Identity & Security et Idemia). Cependant, en matière d'écosystème industriel au sens large impliqué dans les développements autour de l'IA, la France est de loin distancée par les Etats-Unis et la Chine qui bénéficient de leur fort tissu industriel du numérique. On observe notamment une fuite des cerveaux de la France vers les Etats-Unis en la matière, qui menace les positions françaises à l'avenir y compris sur le secteur de la sécurité.

4. *Blockchain*. D'abord associée aux cryptomonnaies et au Bitcoin en particulier, la *blockchain* s'impose comme un nouvel outil indispensable de la Confiance Numérique. Ce protocole enregistre et stocke les transactions sous forme cryptée dans une base de données décentralisée. Les informations sont, de fait, infalsifiables et non modifiables. Registre distribué et sécurisé de transactions, la *blockchain* est à la fois un vecteur de confiance et un outil de lutte contre la fraude. Elle est soit publique (tous les participants peuvent intervenir dans le processus), soit privée. Dans ce cas, seuls certains participants enregistrent des transactions et autorisent ou non leur lecture. Les développements en matière de Confiance Numérique sont multiples : gestion des prestations sociales, protection des infrastructures des opérateurs d'importance vitale, mais aussi missions de sécurité civile ou intérieure et gestion du secret entre institutions.

Ces applications réduiront la dépendance à une autorité centrale mais elles nécessitent l'évolution du système de confiance centralisé actuel vers un système décentralisé pour les applications de type régalien ainsi qu'une nouvelle organisation des opérations. Les acteurs français maîtrisent plusieurs des technologies clés du domaine de la *blockchain* (cryptographie, méthodes formelles…). Cependant, il faut souligner que le niveau d'acceptation de la technologie par les utilisateurs est encore faible. Au niveau mondial, tous secteurs confondus -et bien que ce champ technologique soit encore peu mature l'écosystème industriel américain est clairement le plus avancé dans le développement de solutions intégrant de la *blockchain*. L'écosystème chinois est également important et en très forte croissance. Enfin, les écosystèmes allemand et anglais sont au moins comparables à l'écosystème français.

5. Plateformes d'*Open Hardware/Software* pour l'*edge computing* et les IoTs. Le partage de code logiciel (*Open Software*) est déjà pratiqué depuis un certain temps, mais depuis quelques années, la tendance porte sur le développement du partage du design de composants électroniques (*Open Hardware*). Les logiciels et les matériels en mode *Open Source* accélèrent l'innovation en permettant aux développeurs et aux concepteurs de partager et de réutiliser les développements réalisés par d'autres. La re-publication en *Open Source* des nouveaux développements alimente le processus d'innovation et bénéficie à toute la communauté. Les atouts de la France dans ce domaine de l'*Open Source* sont nombreux. Le marché national est très développé, il représente le quart du marché européen. La communauté tant des chercheurs que des développeurs est sans conteste la plus nombreuse et la plus avancée. Cependant, la sécurité est peu présente dans le monde *Open Source*. Le marché de la sécurité est encore dominé par les grands éditeurs de logiciels propriétaires, nord-américains pour la plupart. Une politique d'achat volontariste et l'incitation au développement de briques technologiques et de plates-formes certifiées et orientées vers l'*Open Source* contribueraient au renforcement de ce domaine, en particulier pour les applications innovantes associées à l'*edge computing* ou aux IoTs pour lesquels la domination américaine ne se fait pas encore trop ressentir.

6. Analyse en temps réel des données d'observations locales et large zone. En matière d'observation et de surveillance locale, l'analyse en temps réel sera à terme la clé de voute du futur écosystème de la vidéosurveillance. Couplée à l'intelligence artificielle, elle permettra d'identifier en temps réel des individus recherchés ou de prendre automatiquement certaines décisions. L'imagerie satellitaire en temps réel se développe également avec de nombreux débouchés en matière d'observation large zone et de renseignement & collecte d'information. La France dispose des acteurs et du savoir-faire technologique pour bénéficier pleinement de ces développements technologiques.

7. D'autres développements technologiques existent, mais qui n'ont pas la même intensité d'impact sur la filière de Confiance Numérique mondiale. Les développements autour de l'identité numérique forment un exemple illustratif : **captcha et challenges pour logiciels, CEV (Cachet Electronique Visible), reconnaissance d'iris, de la forme des veines, mot de passe dynamique…**

6.3 Transformation numérique & miniaturisation : Vers des offres globales de *Security as a Service*

6.3.a La filière de sécurité dans son ensemble est en train de s'uniformiser au niveau de ses produits

En effet, au niveau mondial, la Confiance Numérique est impactée par deux facteurs majeurs :

■ **La miniaturisation couplée à la baisse des coûts des composants électroniques,** conduisant à une croissance toujours plus importante de la part qu'occupent les systèmes ou sous-systèmes électroniques dans les produits de sécurité ;

■ **La transformation numérique,** conduisant à une croissance toujours plus importante de la part qu'occupent les logiciels dans les outils de sécurité. En particulier, les producteurs de produits physiques et électroniques – où les marges sont en moyenne plus basses qu'en cybersécurité – tentent progressivement de monter en gamme dans la chaine de valeur en développant des compétences dans le logiciel. Ces derniers -à l'image de Thales, Idemia ou encore Naval Group- se positionnent de plus en plus fortement sur le développement de logiciels dédiés à des applications de sécurité.

Le croisement des deux tendances décrites ci-dessus conduit donc progressivement les acteurs de la filière industrielle à se positionner sur l'ensemble des segments : physique, électronique et cyber. La distinction physique/électronique/cyber est en conséquence progressivement appelée à avoir de moins en moins de sens et à long terme il est probable que chaque architecture de produit soit globale avec une composante physique, une composante électronique et une composante cyber.

Cette tendance touche même les services privés de sécurité. Alors que la sécurité physique des locaux n'était auparavant composée que de moyens humains, son contenu technologique et électronique s'accroit continuellement (SOC, caméras de vidéosurveillance, etc.), grâce à la miniaturisation et à la baisse des coûts des produits électroniques. Dans la surveillance humaine, la rentabilité nette est très faible (1% en moyenne seulement en 2021 et dopée artificiellement par le CICE). Dans la sécurité électronique, elle est plus élevée, bien qu'avec des niveaux variables selon les entreprises. La volonté d'un grand nombre d'acteurs des services privés est donc de diversifier leurs services en y intégrant des produits électroniques et cyber et en montant en gamme. A titre illustratif, la grande entreprise espagnole Prosegur, l'un des leaders européens du gardiennage, a crée un fonds d'investissement doté de 30 M€ pour investir dans la sécurité électronique et cyber. Depuis 2016, ce fonds a racheté les entreprises Dognaedis, Innevis et Cipher, toutes spécialisées dans la cybersécurité et regroupées au sein de Prosegur sous la marque Cipher. Securitas, autre leader européen de la sécurité privée, a racheté l'activité sécurité électronique de l'américain Stanley Security en janvier 2022 et se développe sur ce segment.

Enfin, cette tendance se ressent également du côté des acheteurs de la filière. Tous les acteurs concernés par des problématiques sécuritaires (et les OIV en particulier), doivent en effet désormais également intégrer la cybersécurité comme un enjeu stratégique. Suez est un exemple emblématique d'acteur traditionnellement concerné par la sécurité à travers la gestion de réseaux d'eau potable et qui considère désormais la cybersécurité comme un enjeu stratégique. Les appels d'offre de digitalisation de la gestion d'eau potable incluent de plus en plus explicitement des volets de cyber-sécurisation des données ainsi générées.

6.3.b Cette uniformisation conduit les industriels à développer de plus en plus d'offres globales clefs-en-main…

Offre globale de cybersécurité clef-en-main, offre globale *Safe City*, offre globale de sécurité, etc. de plus en plus d'acteurs de la filière se positionnent sur ce type d'offre globales en suivant la dynamique d'uniformisation des produits évoquée ci-dessus.

Thales, à travers le rachat de Gemalto en 2019 et la création de la Business Unit « *Digital Identity & Security* » regroupant Gemalto, la Thales Digital Factory, Guavus (spécialiste américain du *Big data analytics* racheté en 2017) et Thales eSecurity (suite au rachat de Vormetric en 2015), est l'exemple le plus emblématique de ce type de stratégie, avec pour objectif de fournir et sécuriser l'ensemble de la chaîne de décision critique en environnement digital. Atos, Orange, Equans et IBM sont également positionnés sur des offres globales.

6.3.c …open source…

Certains acteurs proposent des approches clef-en-main avec systèmes propriétaires. Ces approches sont de moins en moins plébiscitées par les clients qui se retrouvent dépendants d'un unique acteur privé pour l'entretien et l'amélioration future des interfaces. En conséquence, le développement de solutions *open source* se développe de plus en plus.

Dans le domaine particulier des systèmes nationaux de gestion d'identité (état civil) opérés par les Etats, la tendance à l'utilisation de solution en *open source* est aussi perceptible. Toutefois une très forte tendance à la modularité en briques fonctionnelles distinctes s'observe également, car les Etats souhaitent éviter d'être dépendants d'un seul et unique fournisseur ou prestataire pour ne pas en être prisonnier. Elle se traduit en particulier par l'utilisation d'API (*Application Programming Interfaces*) standardisées pour chaque brique fonctionnelle, assurant une indépendance complète dans leur conception, tout en permettant leur interconnexion de manière interopérable. Cette tendance se combine à celle de l'*open source*, car les briques fonctionnelles se reposent de plus en plus sur des solutions open sources. Cette problématique de standardisation d'API prend de l'ampleur sur de nombreux sujets, par exemple avec le concept d'*Open-Services Cloud* (OSC) visant à rendre interopérables les services cloud, réduisant la dépendance des utilisateurs cloud vis-à-vis des *hyperscalers* (voir l'étude de DECISION Etudes & Conseil réalisé début 2023 sur le sujet : Open-Services Cloud (OSC) Unlock Cloud interoperability to foster the EU digital market).

6.3.d … et *As a Service*

En parallèle, on observe à la fin progressive de l'achat simple de produits (logiciels en mode licence, etc.), et le développement de la vente sous forme de service (SaaS: *Software as a Service*, etc.), guidée par la nécessaire adaptation constante des outils de sécurité pour faire face aux nouvelles menaces dans un contexte d'évolutions technologiques permanentes. En 2020, la fourniture de logiciels en mode SaaS représentait déjà 40% de la valeur totale du marché européen des logiciels d'entreprises (DECISION Etudes & Conseil, SITSI). Cette proportion croit d'année en année et devrait approcher les 80% à horizon 2030.

Du côté des offreurs de solutions, ce changement d'usage n'offre pas de nouveaux marchés ou de débouchés. En revanche, il modifie la façon dont les entreprises conçoivent leurs solutions. En conséquence, il offre une opportunité de rebattre les cartes sur l'ensemble des marchés car les leaders actuels qui ne parviendront pas à refaçonner leurs solutions et les business-models adossés à ces solutions perdront dans les prochaines années leurs positions de leaders.

Du côté des clients, la sécurité devient progressivement une compétence organisationnelle qui se retrouve chez l'ensemble des personnes qui participent à la conception des produits et services, et plus uniquement une fonction distincte et isolée du processus de développement d'applications ou des compétences associées. L'une des conséquences est le développement progressif d'équipes internes dédiées dans chacune des unités opérationnelles chez les clients.

A PROPOS DE L'ACN

L'Alliance pour la Confiance Numérique (ACN) représente les entreprises (leaders mondiaux, PME/TPE, et ETI) du secteur de la Confiance Numérique et notamment celles de l'identité numérique, de la cybersécurité et de l'IA de confiance. La France dispose dans ce domaine d'un tissu industriel très performant et d'une excellence internationalement reconnue grâce à des leaders mondiaux, des PME, des ETI et aux différents acteurs dynamiques du secteur.

On dénombre **2 130 entreprises réalisant en France 17,7 Milliards d'euros de chiffre d'affaires** dans ce secteur en forte croissance (7,6% de croissance annuelle moyenne depuis 2016).

Les 106 membres de l'Alliance pour la Confiance Numérique (ACN), dont 89% de PME/TPE-ETI, représentent 2/3 du chiffre d'affaires des entreprises françaises de la Confiance Numérique dans le monde (fabricants de matériel, éditeurs de logiciels, intégrateurs, services, laboratoires d'évaluation de sécurité, recherche,...).

L'ACN est membre de la FIEEC (Fédération des Industries Electriques, Electroniques et de Communication), est membre associé du Campus cyber et participe activement aux travaux du CSF (Comité Stratégique de Filière) des Industries de Sécurité.

Par ailleurs, l'ACN est également membre fondateur de l'association représentant l'écosystème européen de la cybersécurité : ECSO (*European CyberSecurity Organisation*).

ACN
Alliance pour la confiance numérique

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

Les Membres de l'ACN

Les partenaires de l'ACN

A PROPOS DE DECISION

Depuis 2017, DECISION conduit l'Observatoire de la filière de la Confiance Numérique pour le compte de l'ACN.

DECISION est un cabinet d'études et de conseil spécialisé dans la réalisation d'études économiques (analyse de marchés, prévisions, chaînes de valeur, etc.) et de missions de conseil et de stratégie, dans les domaines :

• Electronique (composants, équipements, systèmes) ;
• Aéronautique, Défense, Sécurité ;
• Electrique, Energies renouvelables et Industrie du future.

Nos clients regroupent des entreprises privées, que cela soit des startups/PME/ETI, des grands groupes industriels, desorganisations professionnelles ou des institutions financières et des fonds d'investissements, mais également les pouvoirs publicslocaux et nationaux (gouvernements, ministères, etc.) ainsi que la Commission Européenne.

En 2009, DECISION initie et conduit la première étude pour la Commission Européenne sur l'industrie de sécurité et est un despartenaires du contrat-cadre (2010-2015) sur l'industrie de sécurité (incluant la cybersécurité) pour la DG ENTR de laCommission Européenne.

DECISION a également effectué depuis les études d'évaluation du poids économique de la filière de sécurité pour le gouvernement français :

• En 2015 sous l'égide du PIPAME (Pôle Interministériel de Prospective et d'Anticipation des Mutations Economiques), structure inter-ministérielle regroupant le Ministère de l'Economie (DGE), le Ministère de l'Intérieur (DMISC) et le SGDSN.
• En 2018 sous l'égide du CoFIS (Comité de la Filière Industrielle de sécurité), regroupant le Ministère de l'Economie (DGE), le Ministère de l'Intérieur (DMISC), le SGDSN, le CICS (Conseil des Industries de la Confiance et de la Sécurité), le GICAT et Milipol.
• En 2020 sous l'égide du Conseil Stratégique de Filière (CSF) des Industries de Sécurité, regroupant le Ministère de l'Economie (DGE), le Ministère de l'Intérieur (DMISC), le SGDSN, le CICS (Conseil des Industries de la Confiance et de la Sécurité), et le GICAT.
• En 2022, à travers un consortium regroupant le GICAT, l'ACN, le Ministère de l'Intérieur, le Ministère de l'Economie (DGE) et le SGDSN.

DECISION
ETUDES & CONSEIL

Design graphique / Theo Broyer Alran & Arthur Pajaud.

English Version Available on :
www.confiance-numerique.fr

Partenariats Presse

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