Observatoire de la Filière de la Confiance Numérique

2021

ACN

Alliance pour la confiance numérique

www.confiance-numerique.fr

Sommaire

Le mot de l'ACN - Alliance pour la Confiance Numérique

Philippe Vannier, Président de l'ACN

En cette année si particulière, marquée par une pandémie mondiale et par des mesures gouvernementales inédites en vue de l'endiguer, l'édition 2021 de l'Observatoire ACN de la Confiance Numérique revêt une importance particulière. Pour toutes les entreprises, cette crise se traduit notamment par une visibilité réduite qui complique le travail d'anticipation. A ce titre, l'Observatoire permet d'apporter un premier éclairage précieux sur le comportement de notre filière dans ce contexte inédit.

Il souligne notamment que le secteur de la confiance numérique s'est montré, en 2020, extrêmement résilient face à cette crise et s'affiche comme un des seuls secteurs à n'avoir pas connu de récession en 2020, avec une croissance soutenue de 6,4%, en 2020, du chiffre d'affaires en France de la profession ainsi porté à 13,4 milliards d'euros (généré par plus de 69000 salariés).

Ce constat vient confirmer trois caractéristiques constantes relevées à travers chaque édition de cet Observatoire à savoir que le secteur est durablement dynamique (il bénéficie sur la période 2015-2020, de la plus forte croissance parmi toutes les autres filières en France), créateur de richesse (avec un taux de valeur ajoutée de 47% en 2020, le secteur confirme sa position de filière la plus productive) et riche d'un tissu économique national composé à la fois de grands groupes leaders mondiaux, de PME-ETI très solides, de nombreuses start up agiles et innovantes ainsi que d'une recherche académique de pointe.

Au-delà du constat de l'importance et de la résilience de la filière de la Confiance numérique, cet Observatoire vient surtout souligner les perspectives majeures qui sont autant de défis à relever pour nos entreprises. La crise du Covid a mis en évidence le caractère vital du numérique pour faire fonctionner l'économie et plus largement la société. Elle a tout autant mis en évidence la dépendance de notre pays à des outils, services ou infrastructures numériques de pays tiers.

Au sortir de cette crise, nous évoluerons dans un nouveau paradigme dans lequel les concepts de souveraineté numérique nationale et d'autonomie stratégique européenne sont des enjeux cruciaux. Par ailleurs, cette explosion des usages numériques a généré une augmentation exponentielle de la surface d'attaque favorisant la multiplication d'actes cybermalveillants tels que les rançongiciels. Les pouvoirs publics ont d'ailleurs pris la pleine mesure de ces nouveaux défis tant au niveau national avec la stratégie nationale de cybersécurité volontariste mise en place par le Président de la République, qu'au niveau européen avec une activité législative intense sur tous les aspects liés au numérique.

Ce nouveau paradigme confère à notre filière un rôle majeur : permettre à notre société de bénéficier des apports du numérique en toute confiance et d'être à la pointe de l'innovation tout en en assurant tant la sécurité des données que les libertés fondamentales de nos concitoyens. La maîtrise de notre avenir numérique ne sera possible que si l'ensemble des utilisateurs (Etat, entreprises – depuis les Opérateurs d'Importance Vitale jusqu'aux plus petites PME - TPE - collectivités territoriales mais aussi citoyens) s'approprie les solutions des entreprises de la confiance numérique. Elles sont prêtes et mobilisées pour répondre à cet enjeu décisif.

ACN

Alliance pour la confiance numérique

Le mot de la Direction Générale des entreprises

Thomas Courbe, Directeur général des entreprises

Le secteur du numérique est clé pour le développement et le rayonnement économique de la France, c'est pourquoi l'action du Gouvernement en la matière a connu une très forte actualité depuis le début de l'année 2021. Cette action s'articule autour de trois priorités. La première est de faire de la France et de l'Europe des leaders des technologies du numérique. La seconde est de renforcer notre autonomie stratégique dans le numérique sur les segments critiques pour notre souveraineté. Enfin, alors que la défiance envers le numérique se développe (diffusion de contenus illicites, usage frauduleux des données, impact environnemental), la troisième priorité est d'assurer la cohérence entre nos objectifs sociétaux, éthiques et économiques. Parmi les mesures mises en place pour atteindre ces objectifs, deux stratégies d'accélération du plan de relance contribuent spécifiquement à renforcer la confiance dans le numérique : elles portent sur la cybersécurité et le cloud.

La stratégie d'accélération cyber, annoncée par le président de la République le 18 février 2021, poursuit des objectifs ambitieux à horizon 2025 : multiplier par 3,5 le chiffre d'affaires de la filière pour le porter à 25 Mds€, doubler le nombre d'emplois de 37 000 en 2019 à 75 000 en 2025, ainsi que faire émerger 3 licornes dans le domaine à horizon 2025. Pour atteindre ces objectifs, elle vise à développer des solutions souveraines et innovantes de cybersécurité, à renforcer les synergies entre les acteurs de la filière, à soutenir la demande et enfin à former plus de jeunes et professionnels aux métiers de la cybersécurité, dont le marché de l'emploi est fortement en déséquilibre.

La stratégie cloud du gouvernement présentée le 17 mai s'articule quant à elle autour de trois axes : un label « cloud de confiance » délivré par l'ANSSI visant à garantir une immunité maximale vis-à-vis des lois extraterritoriales, le recours au cloud par défaut pour les nouveaux projets numériques de l'Etat, et enfin la stimulation de l'offre de cloud souverain grâce à une stratégie d'accélération dédiée.

L'observatoire de la confiance numérique est un outil clé pour orienter ces différentes mesures en établissant un état des lieux précis et évolutif de l'environnement des acteurs de la filière. Il permet de révéler des tendances de fond et d'appréhender les différents volets numériques des industries de sécurité en apportant des éléments non seulement sur le secteur de la cybersécurité, mais aussi sur ceux de la sécurité et l'identité numérique. Je salue le travail de l'ACN pour la mise en place de cet observatoire, mais aussi pour sa contribution à la fédération de la filière. C'est un enjeu clé pour permettre à la puissance publique de faire masse des initiatives de l'ensemble des parties prenantes. Une telle approche collaborative est parfaitement alignée avec les objectifs du conseil national de l'industrie dans lequel s'inscrit le contrat stratégique de filière des industries de sécurité, et constitue un levier essentiel pour atteindre les objectifs ambitieux que nous nous fixons collectivement.

MINISTÈRE
DE L'ÉCONOMIE,
DES FINANCES
ET DE LA RELANCE

Liberté
Égalité
Fraternité

Éléments clés

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 2021, couvrant le champ de la cybersécurité et de la sécurité numérique.

La Confiance Numérique en France en 2020 c'est :

- **13,4 milliards d'euros de chiffre d'affaires**, soit 6,4% de croissance entre 2020 et 2019
- **6,5 milliards d'euros de valeur ajoutée**
- **69 200 personnes employées** dans le secteur
- Un **chiffre d'affaires** réparti à **62% pour la Cybersécurité et à 38% pour la Sécurité Numérique**

Les entreprises françaises de la Confiance Numérique dans le Monde en 2020 c'est :

- **21,4 mds € 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 D&S, Atos), de la gestion des identités et des accès (Thales, Idemia, IN Groupe), des services de cybersécurité (Thales, Atos, Orange Cyberdefense, Cap Gemini, Sopra Steria), et de la sécurisation des paiements (Atos)
- **12,6 milliards d'euros de chiffre d'affaires à l'international**, soit 60% du CA total
  (CA exporté depuis la France et CA réalisé à l'étranger par des entreprises détenues par des capitaux français)
- **4,6 milliards d'euros de chiffre d'affaires à l'exportation depuis la France**, soit un taux d'export moyen de 34%

La Confiance Numérique est une filière à part entière :

- **8,1%** de croissance moyenne annuelle en France sur la période 2015-2020, contre **-1,8%** pour le PIB français
- La Confiance Numérique est la f**ilière industrielle française qui bénéficie de la croissance la plus forte depuis 10 ans**
- **La Confiance Numérique s'est montrée particulièrement résiliente face à la crise de la COVID**, avec 6,4% de croissance en 2020 contre -8,3% pour le PIB français. C'est la filière qui réalise la meilleure performance en 2020 avec l'industrie pharmaceutique
- 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 :

- **2 158 entreprises** dans la filière en France
- Dont **74 grandes entreprises**
- Dont **58 ETI** (Entreprises de Taille Intermédiaire)
- Dont **647 PME** (Petites et Moyennes Entreprises)
- Dont **1 379 micro-entreprises**, générant moins de 2 millions de CA en 2020

Éléments clés

FONDAMENTAUX 2020

CA MONDE	21,4 MDS €
CA HORS DE FRANCE	8,0 MDS €
CA FRANCE	13,4 MDS €
DONT CA EXPORT	4,6 MDS €
VA* FRANCE *Valeur Ajoutée	6,5 MDS €

Source : DECISION Etudes & Conseil

CROISSANCE 2019-2020

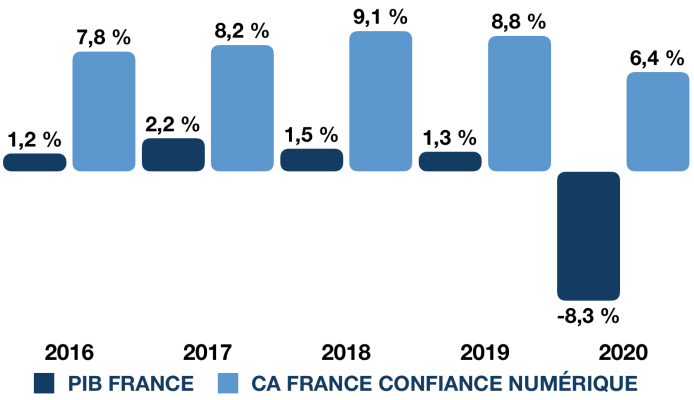
6,4%

69 200 EMPLOIS EN FRANCE

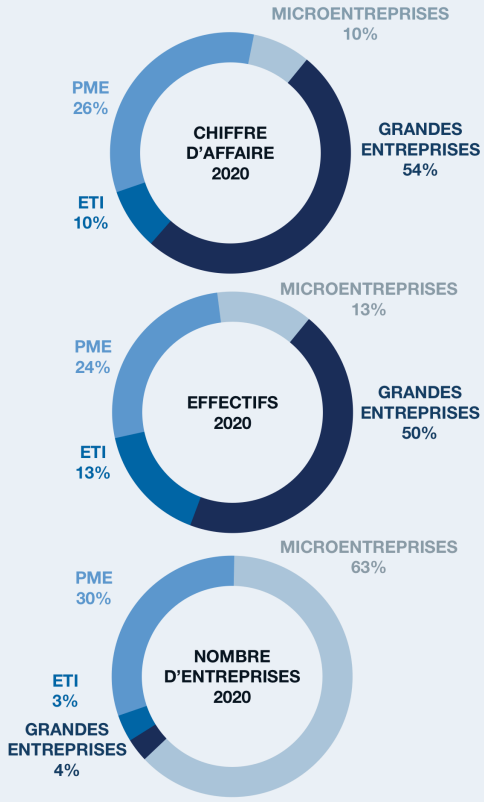
40 000 EMPLOIS A L'ÉTRANGER

CROISSANCE FRANCE COMPARÉES 2016-2020

Source : DECISION Etudes & Conseil

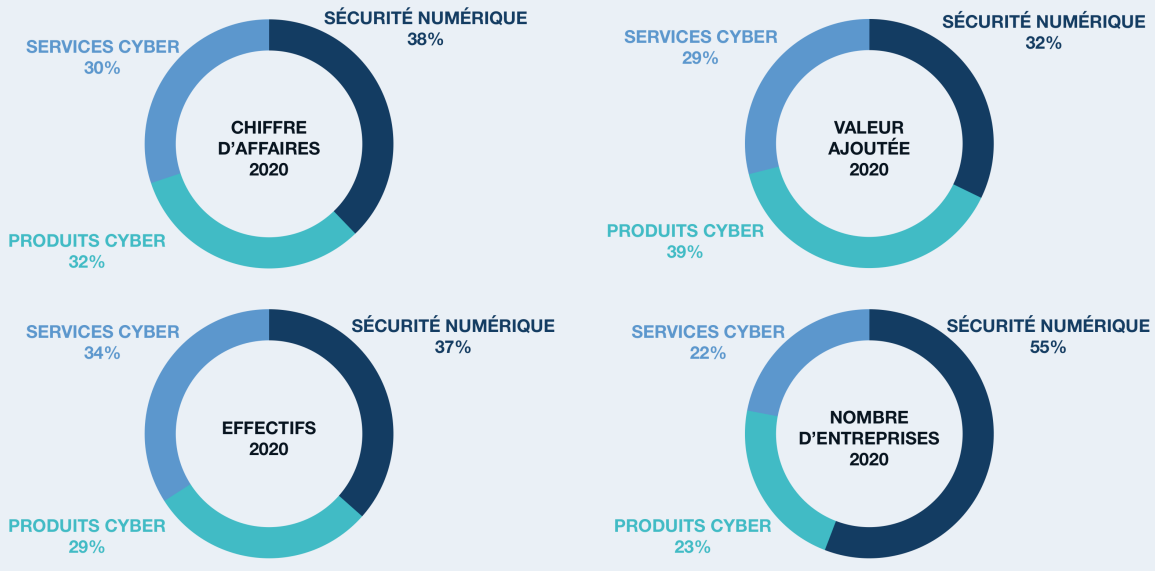


ANALYSE PAR TAILLE D'ENTREPRISES



Source : DECISION Etudes & Conseil

LES PRINCIPAUX SEGMENTS DE LA CONFIANCE NUMÉRIQUE



Source : DECISION Etudes & Conseil

Il s'agit du nombre d'entreprises présentes sur le segment

Éléments clés

TOP 10 ACTEURS FRANCE - 2020

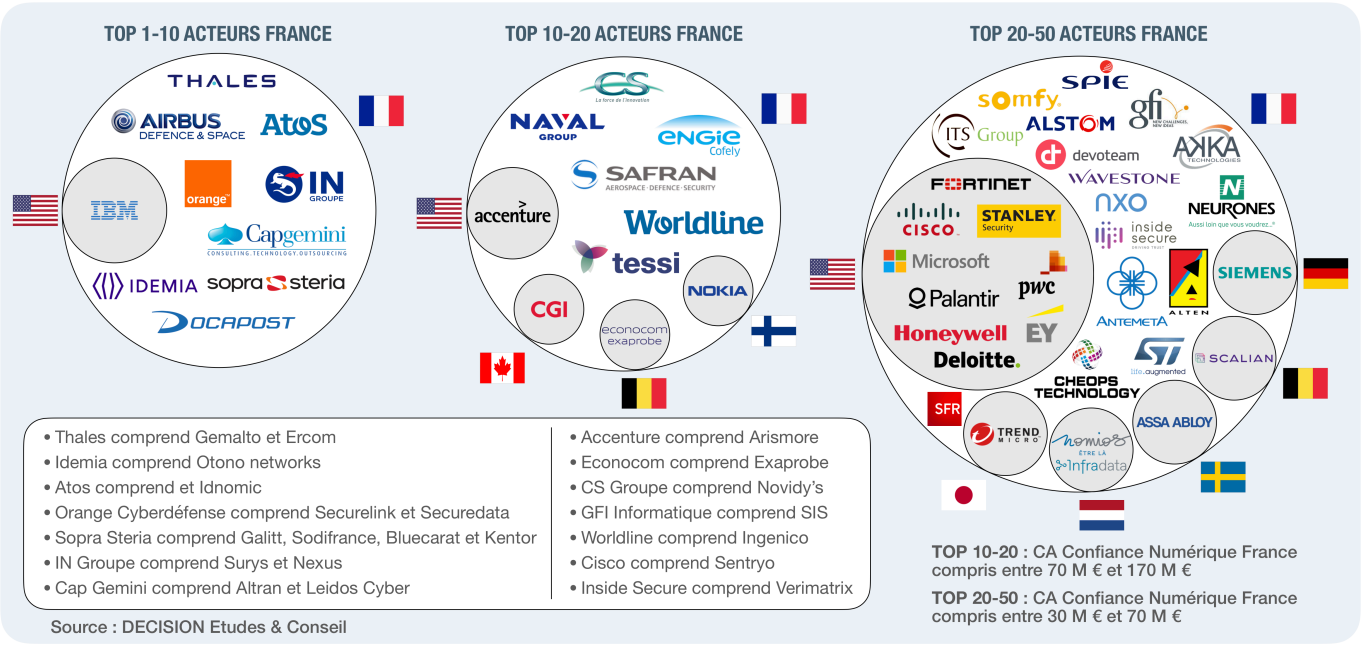
N°	ENTREPRISE	CA CONFIANCE NUMÉRIQUE FRANCE	CA CONFIANCE NUMÉRIQUE MONDE	N° MONDE
1	THALES	1 656 M €	4 384 M €	1
2	AIRBUS D&S	520 M €	727 M €	6
3	ATOS	419 M €	1 028 M €	5
4	IDEMIA	400 M €	2 050 M €	3
5	IBM	313 M €	2 571 M €	2
6	ORANGE CYBERDEFENSE	310 M €	768 M €	7
7	IN GROUPE	290 M €	320 M €	9
8	CAP GEMINI	267 M €	1 307 M €	4
9	DOCAPOSTE	246 M €	246 M €	10
10	SOPRA STERIA	232 M €	564 M €	8

Source : DECISION Etudes & Conseil

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

- **Thales** a créé un leader mondial de la sécurité digitale avec le rachat de Gemalto en 2019
- **Thales, Idemia** et **IN Groupe** sont des leaders mondiaux de l'identité numérique, de l'identification et de l'authentification
- **Airbus D&S** est l'un des leaders européens en sécurité numérique et mondial en observation large zone
- **Atos**, **IBM**, **Orange**, **Cap Gemini** et **Sopra Steria** sont les 5 leaders français parmi les entreprises de services du numérique (classement SITSI), et sont également dans le TOP 10 français en cybersécurité (avec Thales et Airbus D&S)
- **Docaposte** est également un leader français présent sur plusieurs segments de la sécurité numérique et des produits cyber

L'américain Accenture arrive en onzième position en 2020 avec un CA estimé à 170 M€ en France, en forte croissance. Parmi les acteurs réalisant un CA supérieur à 100 M€ en France, on trouve également les français CS Group, Naval Group, Worldline, Safran et Tessi. Les entreprises situées aux environs de la cinquantième position dans la filière ont des CA France de confiance numérique qui avoisinent tous les 30 M€: Neurones, Computacenter, BT, UTC, SAP, Oracle, Prosegur, Schneider. Enfin, si les acteurs français dominent largement le top 10 de la filière, on trouve parmi les acteurs du top 10-20 et du top 20-50 une plus forte présence d'entreprises étrangères implantées en France.



Source : DECISION Etudes & Conseil

I) Confiance Numérique :
Cybersécurité et Sécurité Numérique

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 :

- 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).
- 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.).

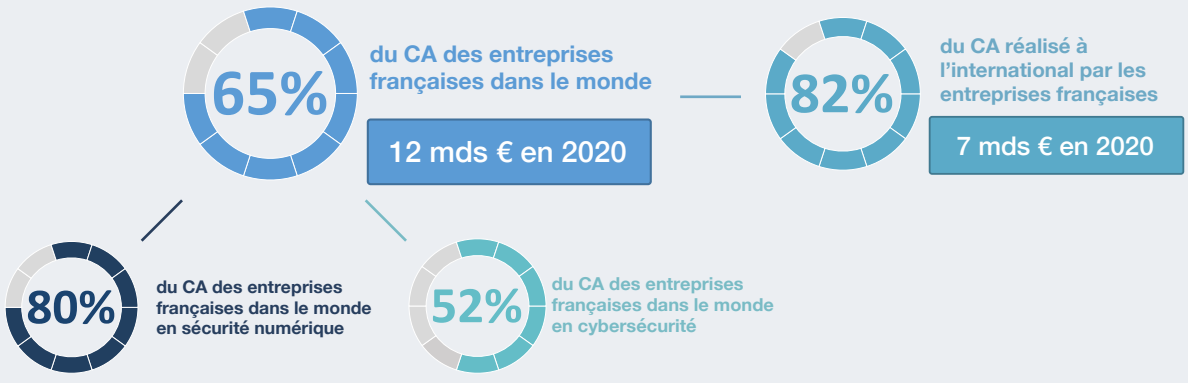
ACN
Alliance pour la confiance numérique

L'ACN est au coeur de la filière

Parmi les adhérents de l'ACN, on trouve :

- **14 grandes entreprises, parmi lesquelles 9 des 10 leaders de la filière en France.**
- Mais aussi **43 PME, TPE et start-ups innovantes adhérents directs** et **plus de 200 PME du secteur** via les écosystèmes de ses membres partenaires (Bretagne Développement Innovation, Pôle SCS, SPAC, FIRST, etc).

Les membres de l'ACN représentent :



I) Confiance Numérique :
Cybersécurité et Sécurité Numérique

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**, correspondants aux systèmes ou sous-systèmes électroniques de confiance ;
- **Les produits de cybersécurité**, correspondant aux développement de logiciels de cybersécurité ;
- **Les services de cybersécurité**, correspondant aux services d'audit, de conseil, et de mise en oeuvre de produits cyber, de sécurisation de l'infogérance ou de formation cyber.

Périmètre de la Confiance Numérique

Sécurité Numérique

Contrôle 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 / Imagerie 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)

Commande contrôle Aide à la décision
Gestion de l'information et de la décision / simulations / autre

Renseignement Collecte d'information
Interception / Ecoute / Localisation / Big data / Investigation

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 vulnérabilité / 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 / 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

I) Confiance Numérique :
Cybersécurité et Sécurité Numérique

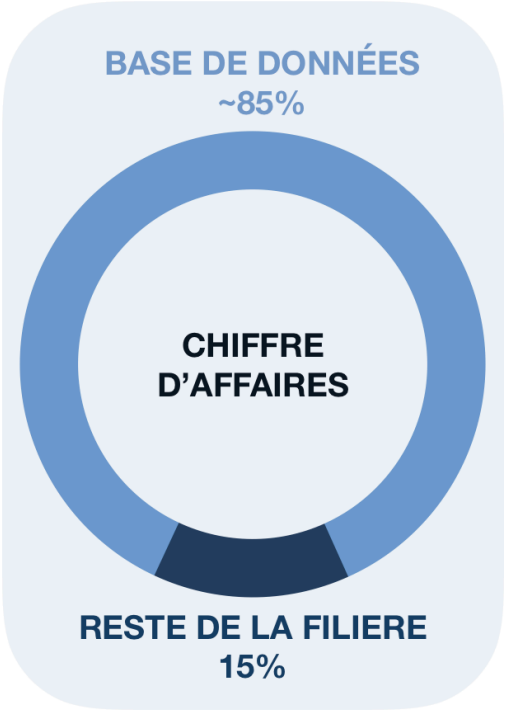
1.3 Méthodologie

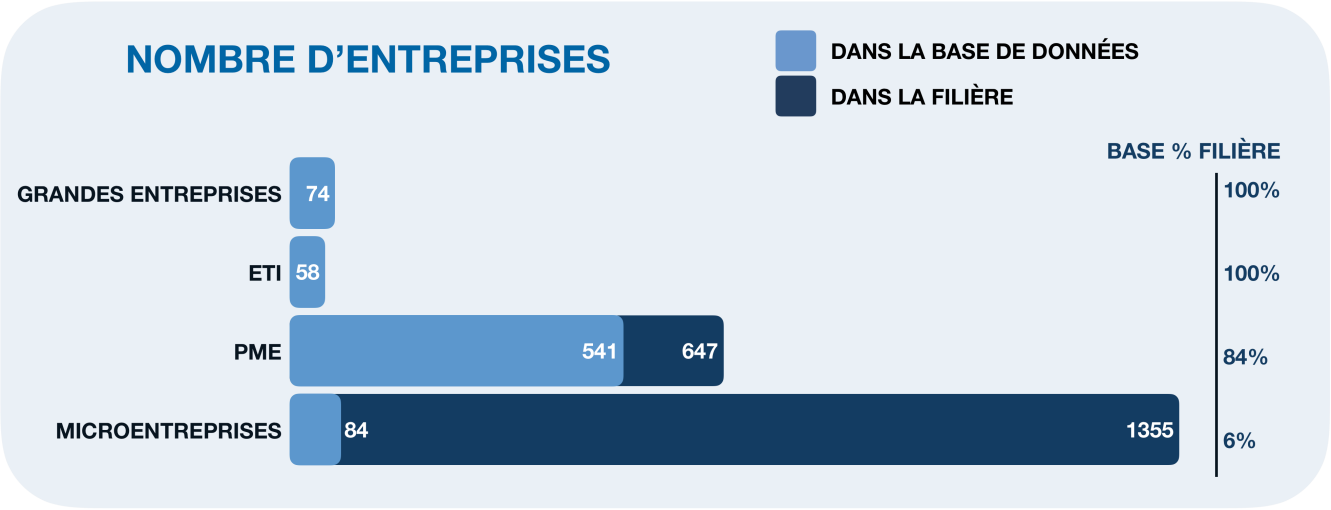
L'objectif de l'Observatoire de la filière de la Confiance Numérique est à la fois de définir le périmètre de la filière et d'en évaluer le poids économique et les caractéristiques.

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 757 entreprises parmi les 2 134 que compte la filière de la Confiance Numérique. Cette base de données prend en compte :

- La totalité des grand groupes de la filière (74/74) ;
- La totalité des entreprises de tailles intermédiaires (ETI) de la filière (58/58) ;
- La majorité des PME de la filière (541/647) ;
- Les micro-entreprises et startups les plus remarquables et innovantes (84/1355).

Ainsi, bien que seul 35% 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.





I) Confiance Numérique :
Cybersécurité et Sécurité Numérique

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 2015-2020 : 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 30% 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 2021, les membres ayant répondu au questionnaire représentent 10% 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 AU PRÉCÉDENTS OBSERVATOIRES

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 2020 et en fonction de la nouvelle segmentation des acteurs. Les chiffres 2019 actualisés sont présentés page 13 de ce rapport.

II) Confiance Numérique :

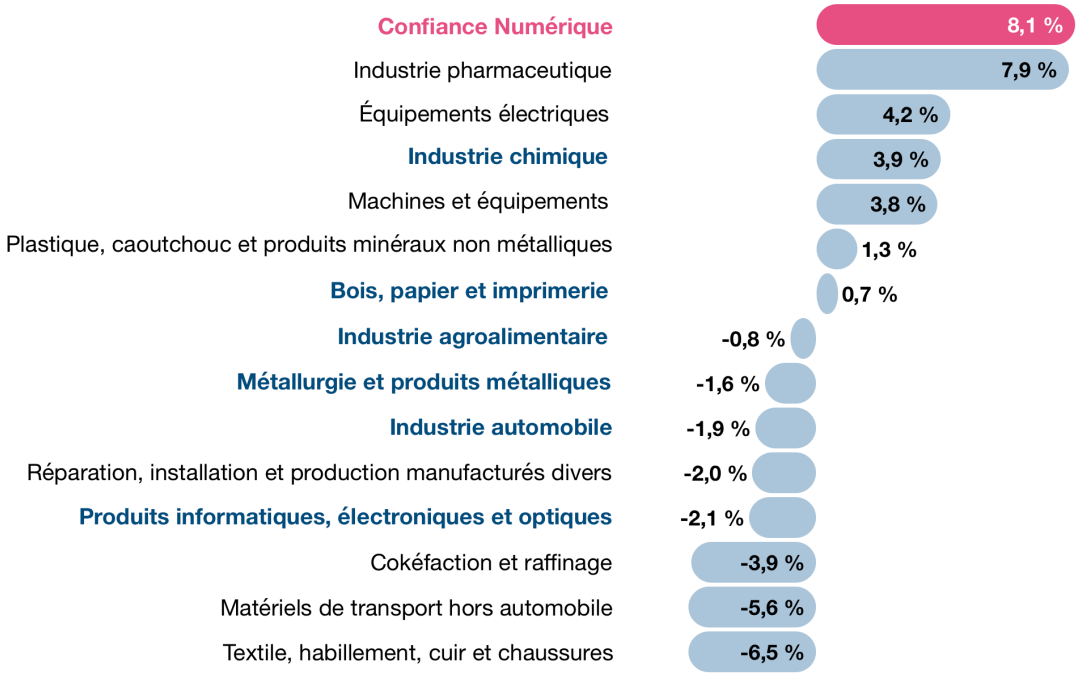
Une filière importante et dynamique

2.1 La Confiance Numérique est l'industrie française qui bénéficie de la croissance la plus forte sur la période 2015-2020

Sur la période 2015-2020, la Confiance Numérique est la filière industrielle avec le plus fort taux de croissance avec 8,1%/an juste devant l'industrie pharmaceutique (7,9%/an). La Confiance Numérique affiche, sur la période, des performances doubles de celles des industries électriques, chimiques ainsi de construction de machines et d'équipements. Les autres industries sont largement distancées, ayant particulièrement souffert de la crise du COVID-19 en 2020.

Cette résilience à la crise traduit des besoins pérennes en biens et services de Confiance Numérique. Si bien qu'à horizon 2025, la Confiance Numérique pourrait devenir la 12ème filière industrielle française sur 15 en valeur ajoutée en dépassant la filière des équipements électriques et des produits informatiques, électroniques et optiques. A horizon 2030, la filière de la Confiance Numérique pourrait dépasser la filière bois, papier et imprimerie et pourrait également rattraper et dépasser en valeur ajoutée l'industrie automobile.

CROISSANCE ANNUELLE MOYENNE DES FILIÈRES FRANÇAISES SUR LA PÉRIODE 2015-2020



Sources : DECISION, Eurostat, OCDE

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)

II) Confiance Numérique :

Une filière importante et dynamique

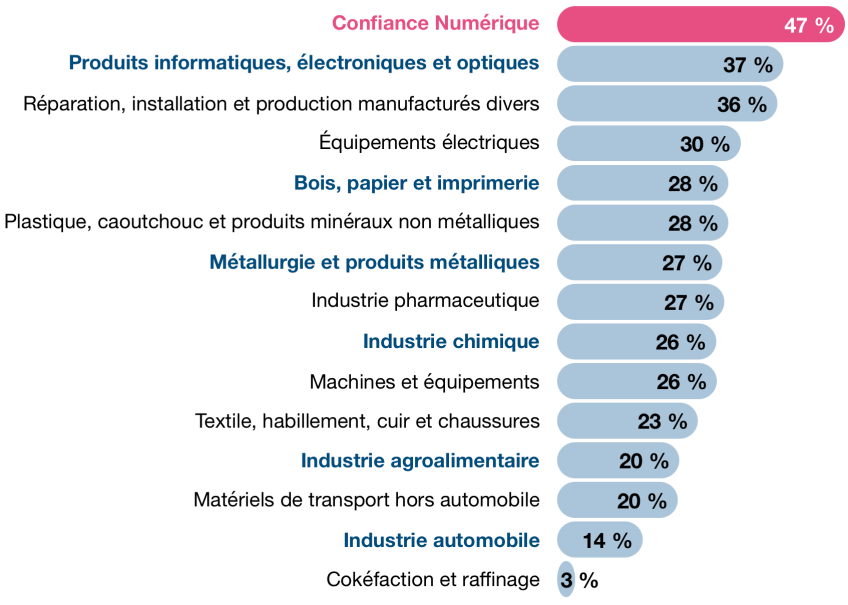
2.2 La Confiance Numérique est la filière industrielle dont l'activité est la plus créatrice de richesse en France

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** (30% en 2020), 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 ils utilisent très peu de consommations intermédiaires et correspondent presque exclusivement à de la transformation des produits au cours de l'activité. Ce phénomène explique en partie le taux élevé de valeur ajoutée de la filière. Cependant, ce phénomène ne justifie par 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 38% du chiffre d'affaires total de la filière de 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 32% 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 FRANÇAISES EN 2020



Sources : DECISION, Eurostat, OCDE

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)

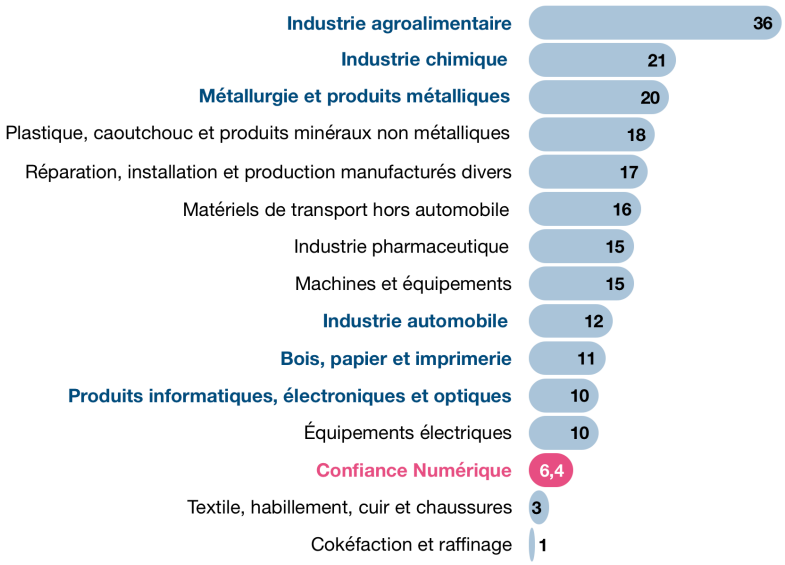
II) Confiance Numérique :

Une filière importante et dynamique

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

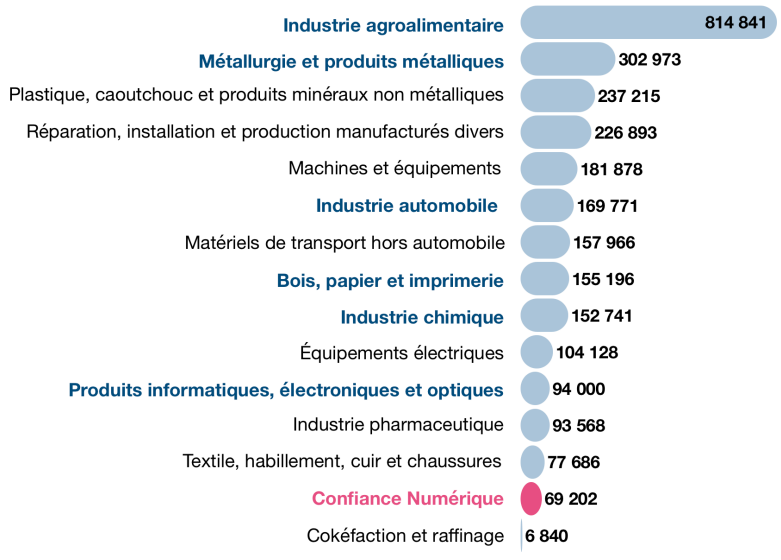
La Confiance Numérique est une filière industrielle à part entière. En termes de valeur ajoutée, elle dépasse significativement les filières de cokéfaction et raffinage ainsi que celle du textile et de l'habillement et se rapproche de l'industrie des équipements électriques. En termes d'emploi, elle dépasse largement la filière de cokéfaction et raffinage et se rapproche rapidement de l'industrie du textile.

VALEURS AJOUTÉES DES FILIÈRES FRANÇAISES EN 2020 (MDS €)



Sources : DECISION, Eurostat, OCDE

EMPLOIS DES FILIÈRES FRANÇAISES EN 2020



Sources : DECISION, Eurostat, OCDE

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)

II) Confiance Numérique :

Une filière importante et dynamique

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 sont positionnées 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 GAFA installent des centres de recherche et débauchent de nombreux talents français. Du côté de la R&D publique, l'INRIA met en place des équipes mixtes composées à la fois d'informaticiens spécialisés dans le deep learning et de mathématiciens fondamentaux. Ces équipes sont dédiées en particulier 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 une dizaine d'année, 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 propre 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 digitale**. Accélérée par la crise du COVID-19 en 2020, les entreprises et administrations du monde entier digitalisent leurs processus et interconnectent les réseaux de données. Cette transformation génère de la croissance auprès des industries de sécurité pour deux raisons. D'une part, la cybersécurité devient assurément un enjeu stratégique majeur pour chaque organisation. D'autre part, les réseaux de données générées par la transformation digitale peuvent être utilisés à des fins de sécurité par des logiciels dédiés innovants (notamment en matière d'identification et d'authentification) ;
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 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.

II) Confiance Numérique :
Une filière importante et dynamique

2.6 Une concurrence croissante de la part des acteurs étrangers

Les acteurs de nationalité française génèrent 77% du chiffre d'affaires de la Confiance Numérique en France, soit 10,3 milliards d'euros en 2020. Autrement dit, l**es acteurs étrangers de la filière réalisent 23% du chiffre d'affaires de la filière en France**, soit environ 3,1 milliards d'euros en 2020. 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.

De même que pour la production en France, le poids des acteurs étrangers sur le marché français est important : il est estimé entre 30% et 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 sont également signalés dans la plupart des segments de la Confiance Numérique sur la période 2013-2021. Parmi les rachats significatifs, figure 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) et fusionné avec Oberthur Technologies sous la marque Idemia en 2018. Début 2021, deux pépites françaises se sont faites racheter par des entreprises américaines : Alsid (sécurisation des environnements) rachetée par Tenable pour 98 M$, puis Sqreen (sécurité des applications), racheté par Datadog.

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 (-1,8%/an de croissance du PIB français sur la période 2015-2020), 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 (Opérateur d'Importance Vitale), et/ou des OSE (Opérateur de Service Essentiel).**

Le triptyque standardisation, certification et prescription 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 :

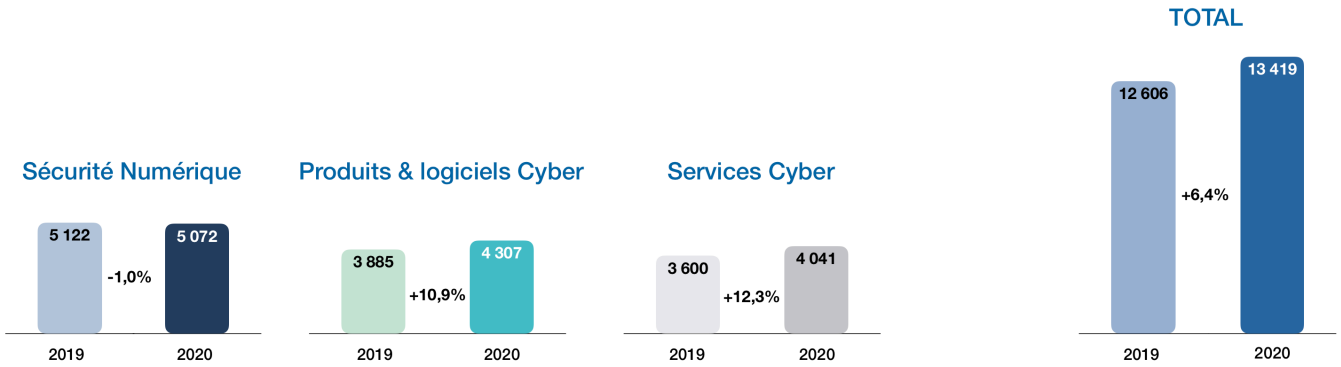
- Le **potentiel de croissance** est durablement supérieur à celui de toutes les autres industries françaises ;
- La Confiance Numérique est déjà de **taille significative** ;
- Les acteurs français sont à la pointe en matière de **compétences et de R&D** ;
- Ce secteur est essentiel à la **souveraineté 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.

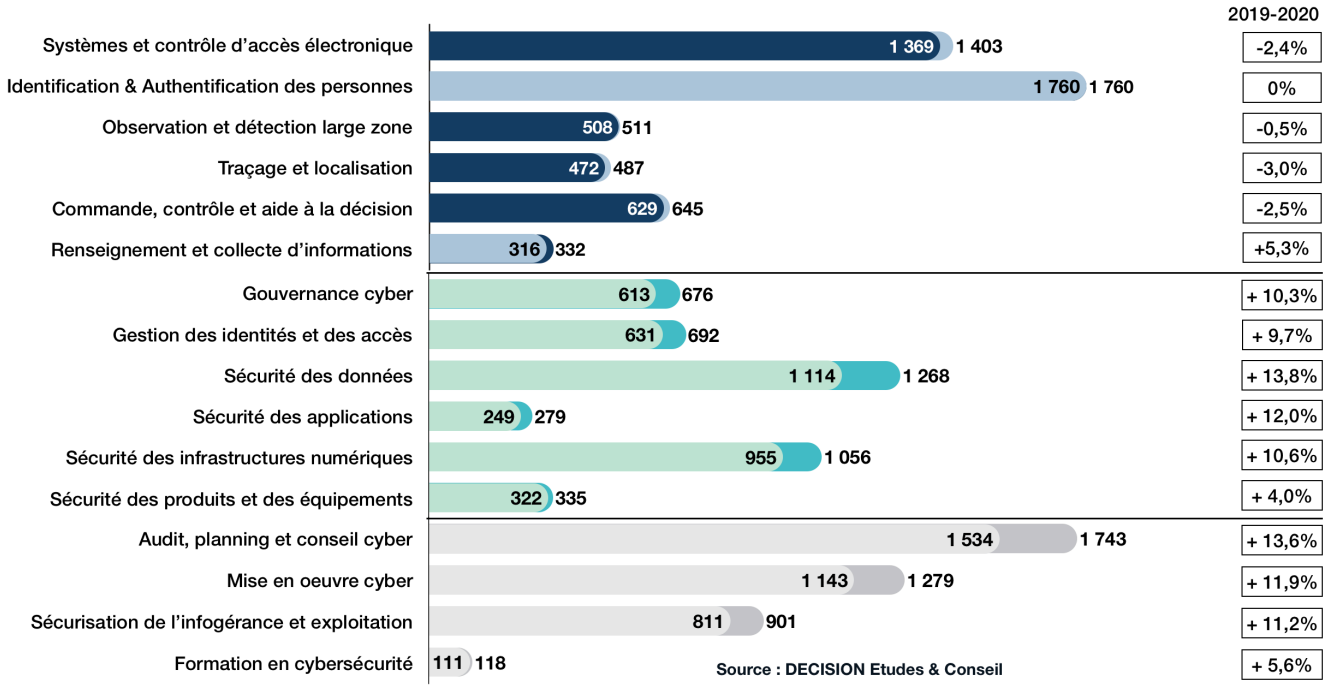
III) Les chiffres clés de la filière

3.1 Taille et croissance

CA de confiance numérique en France : 13,4 Mds € en 2020



Source : DECISION Etudes & Conseil



Source : DECISION Etudes & Conseil

III) Les chiffres clés de la filière

3.2 Valeur Ajoutée

VALEUR AJOUTÉE EN FRANCE EN 2020 PAR SEGMENT

SÉCURITÉ NUMÉRIQUE

2 083 M€

+

PRODUITS DE CYBERSÉCURITÉ

2 516 M€

+

SERVICES DE CYBERSÉCURITÉ

1 877 M€

=

N°	SEGMENT	VALEUR AJOUTÉE EN 2020 EN MILLIONS D'EUROS
1.2.1.1	CONTROLE D'ACCES	510
1.2.1.2	IDENTIFICATION & AUTHENTIFICATION DES PERSONNES	692
1.2.6	OBSERVATION ET DETECTION LARGE ZONE	271
1.2.7	TRAÇAGE ET LOCALISATION	178
1.2.9	COMMANDE, CONTRÔLE ET AIDE À LA DÉCISION	291
1.2.10	RENSEIGNEMENT ET COLLECTE D'INFORMATION	142
2.0.1	GOUVERNANCE CYBER	387
2.0.2	GESTION DES IDENTITÉS ET DES ACCÈS	441
2.0.3	SÉCURITÉ DES DONNÉES	765
2.0.4	SÉCURITÉ DES APPLICATIONS	193
2.0.5	SÉCURITÉ DES INFRASTRUCTURES NUMÉRIQUES	599
2.0.6	SÉCURITÉ DES PRODUITS & ÉQUIPEMENTS	131
3.0.1	AUDIT, PLANNING ET CONSEIL CYBER	715
3.0.2	MISE EN OEUVRE CYBERSÉCURITÉ	554
3.0.3	INFOGÉRANCE - EXPLOITATION	537
3.0.4	FORMATION EN CYBERSÉCURITÉ	71

Source : DECISION Etudes & Conseil

6 476 M€ DE VA DE CONFIANCE NUMÉRIQUE EN FRANCE

3.3 Emplois

EMPLOIS EN FRANCE EN 2020 PAR SEGMENT

SÉCURITÉ NUMÉRIQUE

25 275

+

PRODUITS DE CYBERSÉCURITÉ

20 343

+

SERVICES DE CYBERSÉCURITÉ

23 584

=

N°	SEGMENT	EMPLOIS EN 2020
1.2.1.1	CONTROLE D'ACCES	6 361
1.2.1.2	IDENTIFICATION & AUTHENTIFICATION DES PERSONNES	8 500
1.2.6	OBSERVATION ET DETECTION LARGE ZONE	2 481
1.2.7	TRAÇAGE ET LOCALISATION	2 368
1.2.9	COMMANDE, CONTRÔLE ET AIDE À LA DÉCISION	3 292
1.2.10	RENSEIGNEMENT ET COLLECTE D'INFORMATION	2 273
2.0.1	GOUVERNANCE CYBER	4 059
2.0.2	GESTION DES IDENTITÉS ET DES ACCÈS	2 927
2.0.3	SÉCURITÉ DES DONNÉES	5 790
2.0.4	SÉCURITÉ DES APPLICATIONS	1 166
2.0.5	SÉCURITÉ DES INFRASTRUCTURES NUMÉRIQUES	5 030
2.0.6	SÉCURITÉ DES PRODUITS & ÉQUIPEMENTS	1 371
3.0.1	AUDIT, PLANNING ET CONSEIL CYBER	10 659
3.0.2	MISE EN OEUVRE CYBERSÉCURITÉ	7 818
3.0.3	INFOGÉRANCE - EXPLOITATION	4 116
3.0.4	FORMATION EN CYBERSÉCURITÉ	991

Source : DECISION Etudes & Conseil

69 202 EMPLOIS DE CONFIANCE NUMÉRIQUE EN FRANCE

III) Les chiffres clés de la filière

3.4 Nombre d'entreprises

NOMBRE D'ENTREPRISES EN FRANCE EN 2020 PAR SEGMENT

SÉCURITÉ NUMÉRIQUE
1 708

PRODUITS DE CYBERSÉCURITÉ
704

SERVICES DE CYBERSÉCURITÉ
690

N°	SEGMENT	NOMBRE D'ENTREPRISES EN 2020
1.2.1.1	CONTROLE D'ACCES	326
1.2.1.2	IDENTIFICATION & AUTHENTIFICATION DES PERSONNES	490
1.2.6	OBSERVATION ET DETECTION LARGE ZONE	192
1.2.7	TRAÇAGE ET LOCALISATION	223
1.2.9	COMMANDE, CONTRÔLE ET AIDE À LA DÉCISION	268
1.2.10	RENSEIGNEMENT ET COLLECTE D'INFORMATION	216
2.0.1	GOUVERNANCE CYBER	208
2.0.2	GESTION DES IDENTITÉS ET DES ACCÈS	207
2.0.3	SÉCURITÉ DES DONNÉES	331
2.0.4	SÉCURITÉ DES APPLICATIONS	159
2.0.5	SÉCURITÉ DES INFRASTRUCTURES NUMÉRIQUES	332
2.0.6	SÉCURITÉ DES PRODUITS & ÉQUIPEMENTS	158
3.0.1	AUDIT, PLANNING ET CONSEIL CYBER	626
3.0.2	MISE EN OEUVRE CYBERSÉCURITÉ	440
3.0.3	INFOGÉRANCE - EXPLOITATION	345
3.0.4	FORMATION EN CYBERSÉCURITÉ	211

Remarque : Il s'agit du nombre d'entreprises présentes sur le segment
Source : DECISION Etudes & Conseil

2 158 ENTREPRISES DE CONFIANCE NUMÉRIQUE EN FRANCE

IV) Les tendances de marché

4.1 L'impact de la crise du COVID en 2020

4.1.a. Une industrie résiliente face à la crise

La série de diagrammes ci-contre permet de comparer la croissance de la Confiance Numérique en France en 2020 avec celle des autres industries manufacturières françaises.

> **Remarque** : Les chiffres estimés dans cet Observatoire pour la Confiance Numérique ne sont pas directement comparables avec les chiffres de croissance de l'INSEE présentés ici. En effet, cet observatoire mesure la croissance du *chiffre d'affaires* tandis que les chiffres mesurés par l'INSEE correspondent à la croissance de l'*Indice de Production Industrielle* (IPI)*.

En comparant la Confiance Numérique avec les autres industries manufacturières en 2020, il ressort clairement que la Confiance Numérique est la seule industrie n'ayant pas connu de récession avec l'industrie pharmaceutique malgré la crise du COVID.

Deux principaux facteurs expliquent la résilience de la filière en 2020 :

- **Le secteur public a soutenu la demande**. La demande issue du public (notamment la hausse des budgets de défense à travers le monde) a permis de maintenir de relativement bons niveaux d'activité et d'éviter une récession trop importante dans de nombreux segments, en particulier en sécurité numérique.
- **Une croissance tirée par la cybersécurité**. Mais la principale raison de la bonne performance de la Confiance Numérique en 2020 provient de la cybersécurité qui maintient sa croissance par rapport à 2019 (seulement un point de croissance de perdu par rapport à l'année 2019).

Principaux drivers de la croissance cyber

- Accélération de la croissance « digitale » portée par la crise sanitaire et les besoins accrus de connectivité. Le télétravail a notamment accru l'attention des entreprises autours des problématiques de cybersécurité, de même que l'importance des paiements numériques devant être sécurisés.
- Dématérialisation croissante dans le cloud générant des besoins en authentification et protection des données.
- Augmentation continue des cyberattaques (particulièrement les ransomware en 2020).
- Services de cybersécurité peu impactés par les mesures prises pour endiguer la crise.

La croissance de la Confiance Numérique a en revanche été négativement impactée par la demande issue de l'industrie au sens large et en particulier des industries aéronautiques et automobiles, mais aussi des services de Commerce / Vente / Distribution.

Malgré la crise du COVID, la Confiance Numérique reste donc la filière industrielle qui bénéficie de la plus forte croissance en France sur la période 2015-2020, juste devant la filière pharmaceutique.

* L'Indice de Production Industrielle (IPI), est un outil de suivi du cycle conjoncturel construit sur des enquêtes mensuelles de branches auprès des entreprises ayant des activités industrielles. Ces enquêtes visent à mesurer l'activité productrice des entreprises et, plus précisément le value de la production industrielle. L'IPI étant une donnée mensuelle, la croissance présentée ici est celle de la moyenne annuelle des niveaux bruts de l'indice IPI (base 100 en 2015).

IV) Les tendances de marché

En ce qui concerne la croissance des différents segments de la filière (voir les détails de la croissance par sous-segment en page 13) :

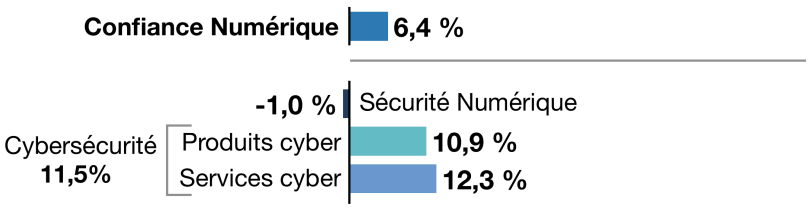
- La **sécurité numérique**, et en particulier les segments du contrôle d'accès, de l'identification et authentification des personnes et du traçage et localisation **ont été affectés par la baisse de la demande associée aux transports et aux voyages, en particulier aériens** (passeports, contrôle d'accès dans les aéroports, etc.).

  Les besoins issus des **services bancaires** ont au contraire **soutenu la demande dans le segment identification et authentification**.

  Les segments du contrôle d'accès et du traçage et localisation ont été négativement affectés par la chute conjoncturelle de la demande issue du secteur privé.

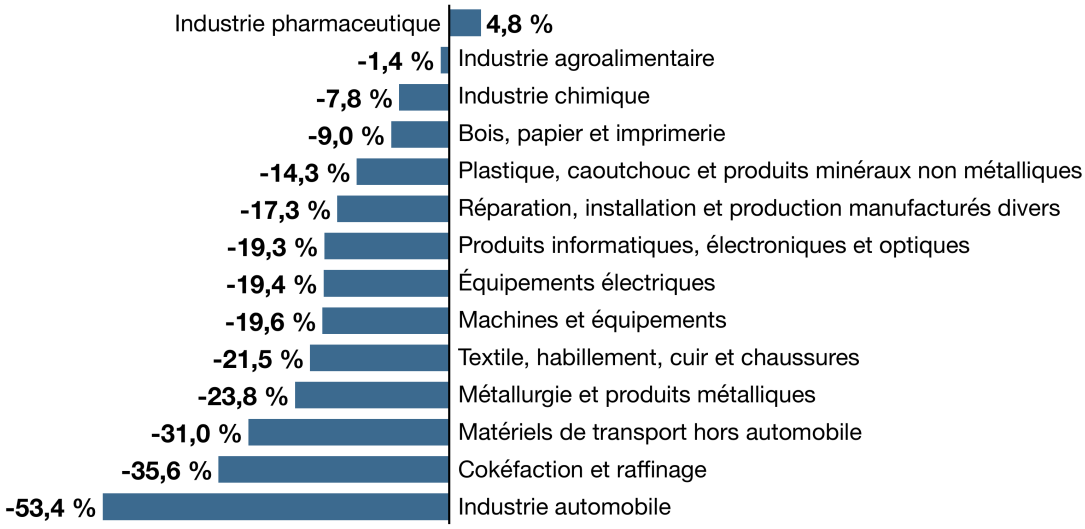
- Les **services de cybersécurité** constituent le seul segment dont la croissance ne diminue pas par rapport à 2019. Elle augmente même (+13,6% contre +11,1% en 2019), soutenue par l'augmentation continue des cyberattaques et par la digitalisation accélérée due au COVID (télétravail, etc.), et peu affectée par les mesures de confinement. Les services de cybersécurité croient à un rythme bien supérieur à celui des services numériques au sens large. Selon le cabinet SITSI, spécialiste des services numériques, le TOP 10 des ESN (Entreprise de Service Numérique) a subit une récession de -2,5% en France en 2020 et une croissance de 4,6% en 2019.

Croissance 2020 du chiffre d'affaires de la filière Confiance Numérique en France



Sources : DECISION Etudes & Conseil

Croissance 2020 des autres filières manufacturières en France (Indice de Production Industrielle)



Sources : INSEE

IV) Les tendances de marché

4.1.b. Perception de l'évolution des marchés par les acteurs de la filière en 2020

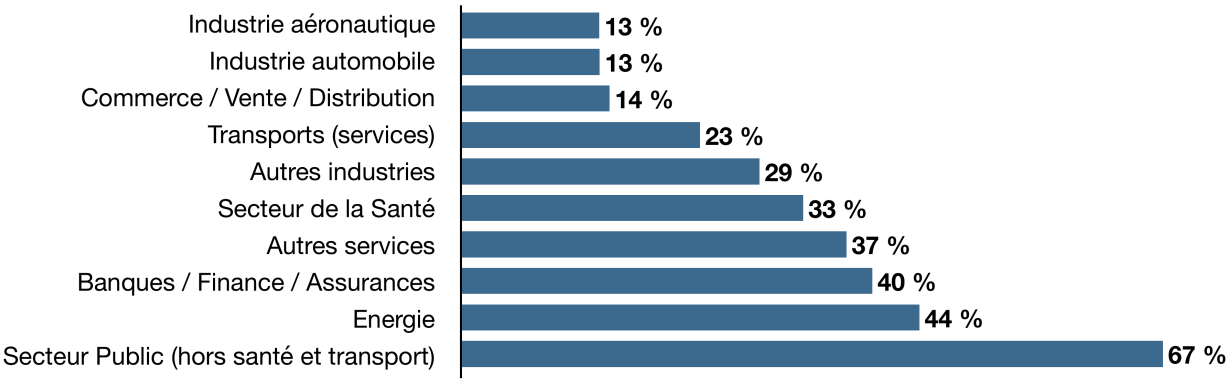
Les trois principaux marchés de la filière sont historiquement l'industrie au sens large, puis le secteur public (administration, forces de sécurité, safe city, collectivités locales, hors santé et transports publics), et le secteur Banque / Finance / Assurance. Parmi les autres marchés de taille significative pour la filière, on trouve les transports (publics et privés), le secteur de l'énergie et des réseaux, et celui de la santé.

Le questionnaire en ligne renseigné par des acteurs représentatifs de 10% de la filière en France (en termes de CA) a permis de collecter le point de vue des entreprises interrogées sur les marchés qui ont le plus soutenu leur croissance en 2020. Les résultats sont présentés dans le diagramme ci-dessous.

Le secteur public, qui compte pour l'un des principaux marchés de la filière, est clairement perçu comme le secteur ayant le plus soutenu la croissance de la filière durant cette année 2020 marquée par la crise.

De façon générale, les marchés qui ont soutenu la croissance de la filière sont ceux qui ont été le moins affectés par les mesures gouvernementales pour faire face à la crise (confinement, télétravail, fermeture des frontières, etc.), répondant souvent à des besoins de « première nécessité » : il s'agit du secteur de l'énergie, de la Banque / Finance / Assurance, de la Santé et des services au sens large (y compris services digitaux).

Quels sont les marchés sur lesquels vous avez connu la meilleure croissance de vos activités Confiance Numérique en 2020 ?



Réponse en % des répondants pondérés par leur poids dans la filière.
L'échantillon représente 10% de la filière en chiffre d'affaires.

Les industries au sens large et en particulier les industries aéronautiques et automobiles ont été les plus touchées, avec le secteur des transports (impacté par les restrictions), et celui du Commerce / Vente / Distribution (impacté par les fermetures).

Par ailleurs, parmi les acteurs interrogés dans le questionnaire en ligne, les seuls marchés sur lesquels certains répondants ont indiqué avoir subit une récession en 2020 sont les marchés :

- Aéronautique.
- Banque / Finance / Assurance.
- Secteur public.
- Energie.

Sur chacun de ces marchés, les répondants ayant indiqué avoir subit une récession en 2020 représentent moins de 30% de l'échantillon en termes de chiffre d'affaires confiance numérique.

Autrement dit, le questionnaire en ligne confirme pour la grande majorité des marchés de la filière confiance numérique, la croissance s'est maintenue en 2020.

IV) Les tendances de marché

4.2 Les évolutions liées à la crise du COVID 19

4.2.a. Évolution des risques et de la menace

La crise pandémique mondiale à laquelle nous sommes confrontés a entrainé des modifications profondes dans nos mode de vie et dans l'ensemble de nos activités sociales et économiques. En quelques jours, le numérique est devenu un lien vital essentiel pour notre société et pour nos entreprises. Qu'il s'agisse d'interagir avec ses proches malgré le confinement, de permettre au tissu économique et aux chaînes d'approvisionnement de maintenir une activité essentielle, ou encore d'optimiser la gestion opérationnelle de la crise, le numérique a fait la preuve de son caractère à la fois stratégique et vital, mais aussi de sa résistance à un choc d'une ampleur historique. La dynamique de numérisation de toutes les activités que nous connaissions avant la crise est ainsi appelée à s'amplifier.

Il est probable, que même lors de la levée définitive des restrictions liées à la pandémie, ce nouveau paradigme ne perdure et ne vienne modifier nos modèles d'avant crise.

Ce constat appelle donc une redéfinition des risques et menaces à l'aune de ce nouveau paradigme. La crise a, par exemple, mis en lumière la dépendance importante de la France et de l'Europe aux infrastructures, applications ou solutions numériques de pays tiers tant au niveau de la capacité d'accès à ces solutions qu'au niveau de leur cybersécurité. Cela conduit à s'interroger sur les conséquences de notre absence de maîtrise sur les maillons de la chaîne de valeur du numérique et sur les risques créés par cette dépendance, notamment en termes de souveraineté numérique.

Par ailleurs, le numérique déploie ses applications dans tous les domaines : c'est sa principale force dans la mesure où ses effets bénéfiques s'en trouvent démultipliés, mais c'est aussi sa principale faiblesse tant il rend le risque systémique. De fait, la numérisation à marche forcée de notre société et de notre économie, a pour corolaire une augmentation exponentielle de la surface d'attaque et de l'exposition aux risques de cybersécurité. Ce constat est particulièrement prégnant concernant le télétravail dont l'usage a explosé durant cette période et dont les conditions de mise en œuvre n'ont que rarement permis un déploiement sécurisé. Désormais, il est urgent de remédier à cette situation et d'augmenter le niveau de sécurité de cette nouvelle pratique du travail afin d'éviter d'exposer les entreprises à de nombreux risques numériques.

L'explosion des rançongiciels est autre une expression visible de l'augmentation des risques : l'ANSSI a publié, le 1er février 2021, un document sur l' « État de la menace rançongiciel à l'encontre des entreprises et institutions » dans lequel il relève une augmentation de 255% du nombre de signalement en 2020 par rapport à 2019 avec des attaques qui sont principalement du Big Game Hunting, du ransomware-as-a-service (RaaS) et de la double extorsion ciblant des collectivités territoriales, le secteur de la santé, le secteur de l'éducation et les Entreprise de Services Numériques (ESN).

La crise du Covid19 a donc accentué des tendances déjà existantes et mis en lumière la nécessité d'apporter des réponses fortes pour renforcer la confiance numérique et préserver notre autonomie stratégique et notre souveraineté numérique.

4.2.b. Une stratégie nationale de cybersécurité

Pour amorcer une réponse à ces constats, le Président de la République française a, le 18 février 2021, annoncé la mise en place d'une Stratégie Nationale pour la cybersécurité l'érigeant ainsi en enjeu stratégique prioritaire.

Parmi les thématiques énoncées dans cette stratégie nationale se trouve notamment le renforcement des liens entre les acteurs de la filière, le soutien de la commande publique aux offres de confiance française et la sensibilisation des collectivités territoriales. Le Président de la République a également insisté sur l'importance de pouvoir s'appuyer sur une offre de cybersécurité souveraine et de confiance et de permettre à l'écosystème de la confiance numérique de se structurer plus fortement et d'être plus visible notamment grâce à la création d'un lieu totem : le Campus Cyber.

IV) Les tendances de marché

Les objectifs de cette stratégie à horizon 2025 sont ambitieux : multiplier par 3,5 le chiffre d'affaires de la filière pour le porter à 25 Mds€, doubler le nombre d'emplois de 37 000 en 2019 à 75 000 en 2025, ainsi que faire émerger 3 licornes dans le domaine à horizon 2025.

Pour compléter ces dispositifs d'actions publique direct et de sensibilisation, l'ACN a proposé la mise en place d'un mécanisme d'incitation financière afin d'aider, l'ensemble des entreprises françaises à envisager des investissements de cybersécurité. Les conditions d'attribution de cet outil incitatif pourraient par ailleurs être adaptées pour que cette sécurisation soit synonyme de souveraineté numérique, par le recours à des solutions de confiance numérique souveraines présentant des garanties de niveau de protection technique et de protection des données personnelles.

« *Créer un dispositif incitatif de type crédit d'impôt cyber doit être considéré par l'État comme un investissement, et non comme un coût. En effet, les sommes investies en accompagnement de la sécurisation, sont à mettre en regard du coût de l'inaction pour la collectivité. Dans le domaine de la cybersécurité, l'anticipation est toujours moins chère que la réaction* » indique Philippe Vannier, Président de l'ACN – Alliance pour la Confiance Numérique, avant d'ajouter : « *Il y a urgence, les entreprises de la filière de la confiance numérique se tiennent à la disposition de l'État pour contribuer à mettre en œuvre de la manière la plus rapide et la plus efficace l'ensemble des dispositifs de cette Stratégie Nationale : il est temps de reprendre en main le contrôle de notre avenir numérique et de garantir notre souveraineté dans ce domaine* ».

4.2.c. Sécurisation du télétravail

L'année 2020 a été marqué par la crise de la Covid 19. Lors du premier confinement, les entreprises ont dû s'adapter extrêmement rapidement à la nouvelle norme du télétravail avec plus de trois millions de « primo-télétravailleurs ». Cette généralisation du télétravail et les différents accès aux systèmes d'informations hors de l'entreprises entraînent de nouveaux risques qu'il s'agit de réduire au maximum. L'actualité illustre chaque jour un peu plus ces nouveaux risques à travers les différentes cyberattaques subies par les entreprises et organisations de toutes tailles, publiques ou privées.

Ces attaques ne s'arrêtent pas uniquement aux services, serveurs ou fournisseurs, elles descendent en cascade sur toutes les infrastructures utilisatrices de ces services. La généralisation du télétravail a mis en avant une vulnérabilité forte aux attaques par périphérie : les attaquants ciblent désormais plus volontiers les télétravailleurs plutôt que le système d'informations de l'entreprise.

Pour permettre une véritable confiance dans le télétravail, les entreprises doivent de leur côté s'adapter à ce nouveau paradigme pour offrir aux salariés la possibilité de travailler à distance tout en maintenant un niveau de sécurité aussi élevé dans ce nouveau contexte. La généralisation du télétravail et les différents accès aux systèmes d'informations hors de l'entreprise entraînent de nouveaux risques qu'il s'agit de réduire au maximum.

Cela implique de repenser et d'adapter les logiques et les processus de sécurisation établis et de porter une attention particulière aux spécificités et aux nouveaux risques induits par l'aspect distanciel notamment sur la sécurisation de l'équipe informatique, la sécurisation du télétravailleur et celle des réseaux et des flux de réseaux.

Notre pays dispose de nombreuses entreprises déployant de solutions souveraines et de confiance pour répondre à ce besoin. L'ACN a récemment entrepris de rassembler et de mettre en lumière ces solutions de confiance, à travers un catalogue des offres du secteur dédiées au télétravail sécurisé, pour aider tous les secteurs à amplifier leur sécurisation.

IV) Les tendances de marché

4.3 Les mouvements de fusion-acquisition

4.3.a. Les champions de la croissance externe

Les principaux acteurs qui se sont développés par croissance externe sur les cinq dernières années sont :

Thales, avec le rachat du leader français Gemalto finalisé en 2019 (Gemalto réalisait un chiffre d'affaires confiance numérique de près de 3 milliards d'euros en 2018 dans le monde). Thales a également racheté en 2019 le français Ercom, qui réalisait un chiffre d'affaires de 12 M € cette année là.

Orange Cyberdéfense, avec le français Lexsi en 2016 (un leader dans les Threat Intelligence Services, totalisant à l'époque près de 20 M € de chiffre d'affaires), l'anglais SecureData en 2019 spécialisé dans les services de cybersécurité et qui réalisait un chiffre d'affaires de près de 50 M€ en 2018, le néerlandais SecureLink en 2019 spécialisé dans les services de cybersécurité et qui réalisait un chiffre d'affaires de 248 M€ en 2018. Soit au total une croissance externe sur la période 2016-2020 de près de 400 M€ au niveau mondial.

Atos a racheté depuis fin 2019 sept entreprises dans le champ de la confiance numérique : le français Idnomic (édition de solutions de PKI), les américains Maven Wave (services cloud et cyber) et Paladion Digital Security (services cyber), l'autrichien SEC Consult Group (services cyber), le canadien In Fidem (services cyber), l'allemand Cryptovision (solutions cryptographiques pour la sécurisation des identités numériques), et la filiale Digital Security du belge Econocom (dédiée aux services de cybersécurité en France, Belgique et Luxembourg). Atos prévoit également le rachat de l'anglais Ipsotek au second semestre 2021 (logiciels de renseignement et analyse d'information). Ces huit entreprises cumulent un chiffre d'affaires confiance numérique estimé entre 180 et 200 M€ dans le monde en 2020. Atos s'est également séparé définitivement de sa filiale Worldline en 2020.

Cap Gemini a racheté en 2019 Altran, qui réalise un chiffre d'affaire important sur le champ de la confiance numérique (estimé à près de 150 M € dans le monde en 2020). Cap Gemini a également racheté la division cyber de l'américain Leidos et ses 500 employés en 2019, représentant un chiffre d'affaires confiance numérique estimé entre 125 et 150 M € en 2020. Ces achats représentent donc environ 300 M€ de croissance externe pour Cap Gemini entre 2019 et 2020 au niveau mondial.

IN Groupe a racheté le français Surys en 2019 puis le suédois Nexus en 2020. Surys est spécialisé dans les solutions optiques de sécurité pour la sécurisation des documents et la traçabilité, et compte près de 400 employés dans le monde. Nexus est un leader européen du marché de l'identité numérique pour les personnes et les objets, et compte 300 employés dédiés à travers l'Europe et l'Inde.

Sopra Steria a racheté une série d'acteurs du conseil numérique comprenant des activités de conseil en cybersécurité entre 2017 et 2020: le suédois Kentor en 2017, l'allemand Bluecarat en 2018 et le français Sodifrance en juillet 2020, dont les activités de cybersécurité cumulées avoisinent aujourd'hui les 50M€. Sopra Steria a également racheté le français Galitt en 2017, spécialisé dans le développement de logiciels sur le marché des systèmes de paiement et des transactions sécurisées. Ces achats représentent plus de 70 M € de croissance externe sur la période 2017-2020 au niveau mondial.

Enfin, l'américain **Accenture** a développé une politique ambitieuse de croissance externe sur le secteur de la cybersécurité au niveau mondial depuis 2015 avec de très nombreux rachats (16 identifiés jusqu'ici) : le français Arismore en 2017, l'ancienne division Cyber Security Service de Symantec rachetée à Broadcom en 2020, mais aussi Fusionx, Cimation, Maglan, Redcore, Defense Point, Endgame Federal Services, iDefense, Deja Vu Security, Context Information Security, Revolutionary Security, et depuis le début de l'année 2021 Openminded et Link by Net. L'ensemble de ces opérations représente près de 2 600 employés venant grossir les rangs d'Accenture sur le segment de la cybersécurité dans le monde. Suite à ces différents rachats, Accenture compte désormais un chiffre d'affaires confiance numérique estimé à près de 3 milliards d'euros dans le monde. Ses activités en France se sont également renforcées et Accenture se situe désormais à la onzième place des entreprises françaises de la confiance numérique, derrière Sopra Steria.

4.3.b. Les mouvements les plus significatifs identifiés depuis 2020

En janvier 2020, **Avisa Partners** a racheté le **CEIS**, après avoir racheté l'allemand **IDA Group** et l'anglais **Gabara Strategies**.

En février 2020, **Worldline** a finalisé l'acquisition d'**Ingenico**, fournisseur de solutions de paiement et de services connexes qui a réalisé un chiffre d'affaires de 3,4 milliards d'euros en 2019 à l'échelle mondiale. Avec Ingenico, Worldline confirme sa position de leader sur le marché du BPO (Bank Payment Obligation) en Europe et entre dans le Top 10 mondial. En outre, Worldline fait désormais partie du Top 5 des fournisseurs de services de paiement BPO à l'échelle mondiale.

En avril 2020, **Data Legal Drive** a racheté son principal concurrent français **Captain DPO** pour se positionner comme une alternative française à l'américain One Trust. Captain DPO réalisait environ 1M€ de chiffre d'affaires avec sa solution logicielle SaaS de gestion de la conformité RGPD.

Docaposte a racheté les français **CDC Arkhinéo** (archivage sécurisé), **AR24** (lettre recommandée électronique) et **Docusign** (identité numérique, signature électronique, etc.) entre mai et octobre 2020. Ces trois entreprises cumulent un chiffre d'affaires confiance numérique de 30M€ en 2020.

En février 2021, deux pépites françaises se sont faites racheter par des entreprises américaines. **Alsid**, spécialiste de la sécurisation des environnements, racheté par **Tenable** pour 98 millions de dollars. Puis **Sqreen**, spécialiste de la sécurité des applications, racheté par **Datadog**.

Enfin, en Mai 2021, **Thales** et **Atos** ont annoncé la création d'une société commune **Athea**. Cette entreprise développera une solution capable d'exploiter des volumes importants de données de façon sécurisée grâce à l'intelligence artificielle. Elle s'adresse aux secteurs de la défense, du renseignement et de la sécurité intérieure. Elle visera tout d'abord le marché français puis s'étendra au marché européen. Le lancement d'Athea est la suite logique pour Thales et Atos qui travaillent déjà ensemble sur le programme Atémis, une plateforme de traitement des données du ministère des Armées français, qui se prépare à entrer en phase d'industrialisation. La création d'une société commune est l'occasion de mutualiser les investissements, les compétences et les expertises des deux entreprises françaises.

4.4 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 impactent la Confiance Numérique de manières différentes et complémentaires.

4.4.a. Les innovations électroniques et numériques qui génèrent de nouveaux marchés

Les innovations issues des industries électroniques et numériques impactent presque tous les secteurs des économie 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 (la production de processeurs de 5 nanomètres sera lancée pour la première fois en 2020 par l'entreprise taïwanaise TSMC et la miniaturisation devrait continuer jusqu'à la « last node » d'un nanomètre à horizon 2025-2030). 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 seuls six entreprises se maintiennent au niveau mondial : Samsung (Corée du Sud), TSMC (Taïwan) et Intel (États-Unis) dans les processeurs et SK Hynix (Corée du Sud), Micron (États-Unis) et Toshiba (Japon) dans les mémoires.

IV) Les tendances de marché

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.

- **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.

Le croisement de ces deux tendances génère de nombreux marchés émergents et porteurs pour la confiance numérique.

1. **Sécurité des objets connectés.** À termes, 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.)… Sur la période 2013-2019, 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. Les progrès dans la standardisation des architectures IoT sont à même d'accélérer la croissance future.

    - **Automobile connectée.** Le principal segment déjà en forte croissance a été 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 sur la période 2013-2019. Les acteurs qui ont le plus bénéficié de la thématique Safe City sont les grands intégrateurs (Thales, Accenture, Cap Gemini, 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 sur la période 2013-2018.

    - **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.** En parallèle du foisonnement technologique en matière d'électronique autour du stockage et du traitement des données (mémoires non-volatiles, 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…).

Thierry Breton, nouveau commissaire européen chargé de la politique industrielle, du marché intérieur, du numérique, de la défense et de l'espace, a fait de la mise en place d'une approche européenne ambitieuse sur les données l'une de ses priorités (données personnelles des utilisateurs internet, unification et protection des données de santé au niveau européen, etc.). Les synergies sont fortes entre le besoin de la France et de l'Europe de protéger leurs données grâce à des solutions souveraines (cloud de confiance public et privé, équipement cyber des hôpitaux et protection des données associées…), et le marché potentiel que cela représente pour la filière de confiance numérique française et européenne -qui dispose des acteurs et des compétences nécessaires pour répondre à cette demande.

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 digitale (« citoyenneté à distance »). La norme actuelle en France demeure l'existence simultanée de nombreuses identités décorrélées, fortes (SIM, cartes bancaires, passeports, etc.), et faibles (identités numériques délivrées très majoritairement par les acteurs du numérique américains du type GAFA pour le e-commerce), sans garantie de protection souveraine des données. L'alternative est le déploiement d'une identité forte unique 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, etc.) et le projet prend forme au niveau français autour du déploiement de la Carte Nationale d'Identité Electronique (CNIe).

   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, logiciels de renseignement et collecte d'information qui bénéficient de larges bases de données générées par le numérique (type Palantir Technologies), etc.

4.4.b. 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.

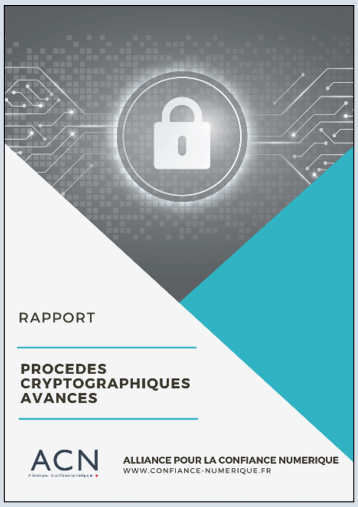
1. **Cryptographie**. La cryptographie regroupe l'ensemble des procédés visant par exemple à chiffrer des informations pour en assurer la confidentialité entre l'émetteur et le destinataire. Les développements technologiques en matière de cryptographie sont très nombreux et l'industrie française comme 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 œuvre dans des environnements restreints, y compris les étiquettes RFID, les capteurs, les appareils de santé et de soins. La cryptographie légère devrait être 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.

IV) Les tendances de marché

- **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 des attaques. Cependant, l'ordinateur quantique et sa puissance de calcul potentielle constituent une menace pour les données chiffrées avec ces méthodes, qu'ils pourraient 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 de sécuriser le transport de l'information.

- **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 devraient émerger à horizon de quelques mois voire quelques années.



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

- **Cryptographie utilisant l'ADN** est 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 sur la période 2023-2030.

- **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 sur la période 2023-2030.

2. **Eléments sécurisés (Secure elements).** Ce domaine innovant est particulièrement important pour la France car toutes les technologies de base connexes y sont nées, permettant le développement de trois leaders mondiaux depuis la France : Thales, Idemia et ST Microelectronics. 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…).

IV) Les tendances de marché

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 & Devaient, 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 regroupe le développement d'algorithmes de machine learning (Réseaux de neurones artificiels, multicouches oui 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 de marche, etc. ;
   - **Conduite de plus en plus autonome des plateformes de sécurité ;**
   - **Agrégation et analyse des données collectées dans les segments de l'observation locale et large zone et du renseignement et collecte d'information ;**
   - L'intelligence artificielle permet la **détection performante en temps réel d'armes et de substances dans un flux de personnes**, dans le segment de la détection de produits dangereux ;
   - **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 d'industriel global 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 pourrait menacer 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 qu'il n'existe pas – encore – de blockchain « made in France » et 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. Les écosystèmes 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 la tendance actuelle porte sur le développement du partage de design de matériel et 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 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, QR codes, reconnaissance d'iris, de la forme des veines, mot de passe dynamique…**

4.5 Transformation digitale & miniaturisation : Vers des offres globales de Security as a Service

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

En effet, au niveau mondial, l'a confiance numérique est impactée par deux facteurs majeurs (déjà évoqués page 23) :

- **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 digitale**, 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 Gemalto (Thales), Idemia ou encore Naval Group- se positionnent de plus en plus fortement sur le développement de logiciels dédiés à des applications de sécurité.

IV) Les tendances de marché

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 jusqu'à récemment 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% à 1,5% seulement sur la période 2013-2016 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 privés des services 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 -et fortement implantée en France- a crée un fond d'investissement doté de 30 M€ pour investir dans la sécurité électronique et cyber. Sur la période 2016-2019, ce fond a racheté les entreprises Dognaedis, Innevis et Cipher, toutes spécialisées dans la cybersécurité et regroupées au sein de Prosegur sous la marque Cipher.

Enfin, cette tendance se ressent également du côté des acheteurs de la filière. De la sécurité à la cybersécurité, tous les acteurs concernés par des problématiques sécuritaires (et les OIVs en particuliers), 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.

4.5.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 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, Engie et IBM sont également positionnés sur des offres globales

4.5.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 leurs conceptions, tout en permettant leurs interconnexions de manière interopérable. Aussi, 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.

IV) Les tendances de marché

4.5.d … et As a Service

En parallèle, la période 2013-2018 est marquée par la fin progressive de l'achat simple de produits (logiciels en mode licence, etc.), et le développement de la vente sous forme de service (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.

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.

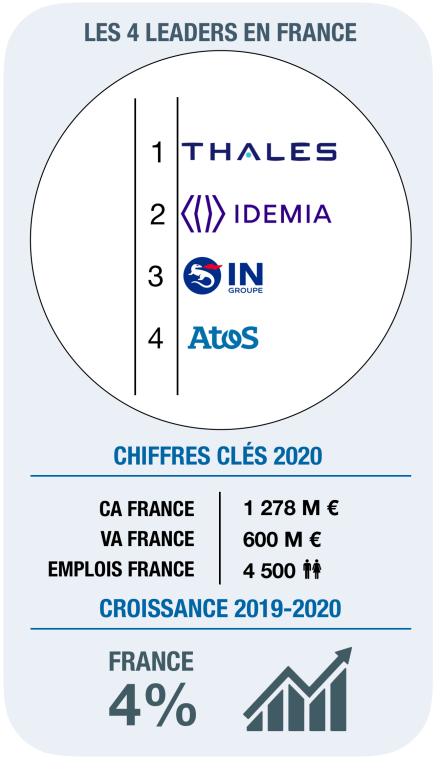
Du côté des clients, la sécurité devient progressivement une compétence organisationnelle qui se retrouve chez l'ensemble des personnes qui participent à la conception des produits et services, et plus uniquement une fonction distincte et isolée du processus de développement d'applications ou des compétences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

4.6 Le potentiel de croissance offert par l'identité numérique

4.6.a. L'identité numérique

L'identité numérique peut se définir comme l'ensemble des processus d'identification électronique (« qui je suis ») et d'authentification électronique (« comment je le prouve »). C'est la clef de voûte de tout service en ligne : sans identité numérique, il n'est pas possible de commercer en ligne, d'avoir accès aux services publics en ligne et donc plus généralement de créer la confiance entre les parties prenantes.

Les enjeux de l'identité numérique sont considérables en matière de souveraineté et de citoyenneté, d'autonomie stratégique, de croissance économique, de transformation numérique de notre société, d'inclusion et de protection des données personnelles, tant du point de vue de l'État que des entreprises. Identifier de manière plus sécurisée les personnes physiques, mais aussi les personnes morales est donc une priorité stratégique.



4.6.b. Un marché mondial porteur

Le développement des usages numériques crée, pour chaque utilisateur, de multiples besoins de s'identifier au quotidien, aussi bien dans la sphère publique (démarches administratives en ligne) que privée (commerce en ligne). Or aujourd'hui, dans la plupart des cas, l'identification sur internet présente un faible niveau de garantie (identifiant et mot de passe), avec un risque quant à l'utilisation des données personnelles, et elle génère de la complexité (comptes multiples).

C'est pourquoi un nombre croissant de pays développent un parcours d'identification numérique unique et sécurisé, pouvant recourir notamment aux données biométriques. Cette identité numérique unique doit permettre à chaque citoyen de s'identifier sur tous les supports utilisateurs. L'Inde fait figure de pionnier en la matière à travers le programme Aadhaar lancé en 2010 qui a permis d'attribuer à toute personne résidant en Inde un identifiant unique associé à ses données biométriques (photographie des iris, du visage, empreintes digitales, etc.), et à son état civil. Toutefois, des approches alternatives sans identifiant unique associé à des données biométriques sont possibles et mises en œuvre de par le monde.

IV) Les tendances de marché

4.6.c. La France, un leader mondial

Les acteurs français sont parmi les leaders mondiaux en matière d'identité numérique, principalement à travers Thales Digital Identity and Security et Idemia, mais aussi à travers IN Groupe (ex Imprimerie Nationale ayant racheté SURYS en 2019), Atos, Worldline ou encore ST Microelectronics.

En conséquence de la présence de ces leaders, le chiffre d'affaires généré en France par l'identité numérique est conséquent : 1,3 milliards d'euros en 2020, pour 4 500 emplois et une valeur ajoutée de 600 millions d'euros.

Voir la brochure capacitaire de l'ACN - Identité numérique publiée en Mars 2019.

4.6.d. Des projets ambitieux en matière d'identité numérique

Le 17 avril 2018, la Commission européenne a publié une proposition de règlement relatif « au renforcement de la sécurité des cartes d'identité des citoyens de l'Union et des titres de séjour délivrés aux citoyens de l'Union et aux membres de leur famille exerçant leur droit à la libre circulation » (Voir la position de l'ACN sur ce projet de règlement).

Le règlement introduit des normes minimales en matière de modèle et de sécurité pour les cartes d'identité. Il rend obligatoire en particulier l'inclusion de données biométriques (visage et empreintes digitales) dans les cartes d'identité des citoyens de l'Union. De plus celles-ci devront être conformes aux spécifications de l'OACI. Le texte a été adopté par le Parlement européen et le Conseil de l'UE en mai 2019. Entre autres, il oblige l'ensemble des Etats-membres délivrant des cartes d'identité à leurs citoyens à émettre des titres conformes aux dispositions de ce texte au plus tard sous deux ans. Ainsi, ce texte constitue une formidable opportunité pour les Etats-Membres d'émettre une nouvelle génération de carte d'identité donnant aussi accès à une identité numérique à son porteur. Il permet donc de renforcer l'impact de l'édifice réglementaire européen en matière d'identité numérique, initié en 2015 par le règlement e-IDAS qui offre notamment un support de reconnaissance des identités numériques entre les Etats européens.

En complément, au niveau national, une mission interministérielle chargée de l'identité numérique a été créée le 5 janvier 2018 par le Ministre de l'Intérieur, la Garde des Sceaux et le Secrétaire d'Etat chargé du Numérique. Elle est confiée à Mme Valérie Péneau, inspectrice générale de l'administration, avec pour objectif de concevoir et de mettre en œuvre un parcours sécurisé d'identification numérique universel et inclusif, plaçant les intérêts des utilisateurs « au cœur [des] démarches ».

Le parcours d'identification numérique proposé par l'Etat vise à comporter au moins deux niveaux de garantie, dont le niveau élevé, au sens du règlement européen e-IDAS qui instaure un cadre commun en la matière et prévoit une obligation de reconnaissance mutuelle des solutions notifiées au sein de l'Union européenne depuis septembre 2018.

Les orientations majeures d'une stratégie française de l'identité numérique sont :

- Faire de la future CNIe (Carte Nationale d'Identité électronique) le support d'une identité numérique de niveau élevé. Elle a commencé à être déployée dans certaines régions, et le sera nationalement à partir d'août 2021.
- S'inscrire dans un écosystème public/privé en facilitant, à partir de cette future CNIe, des offres privées d'identification et en permettant l'accès aux services publics et privés.

Dans la perspective de cet écosystème en construction, divers parcours utilisateurs sont expérimentés afin de mieux appréhender les futurs usages de cette identité numérique. Ces orientations font écho aux attentes formulées par l'ACN en 2012 de mise en place d'une politique nationale de l'identité numérique, « selon une triple exigence de neutralité, d'interopérabilité et de sécurité ». Sur la base de ces orientations, le programme entre désormais dans sa phase opérationnelle, et s'appuie pour ce faire sur les expertises et les compétences d'un tissu industriel national remarquable, dont la capacité en ce domaine est internationalement reconnue.

Ainsi, l'établissement d'une identité numérique française, avec ses aspects régaliens (CNIe) mais surtout sa dérivation sécurisée sur toutes sortes de supports est susceptible d'être, dans les années à venir, un levier fort pour tout un écosystème industriel existant et en cours de création autour des usages, existants ou à venir, de cette identité numérique sécurisé.

Parmi les nouveaux marchés liés à l'identité numérique, ceux dédiés aux personnes morales sont particulièrement notables. Qu'il s'agisse d'identification, de signature électronique ou d'identification des objets et/ou documents (à des fins par exemple de traçabilité ou d'optimisation des processus), de nouveaux usages sont en plein développement. Ces développements se fondent sur des supports technologiques multiples tels que notamment le Cachet électronique Visible (CEV), qui a récemment fait l'objet de travaux de normalisation.

4.7 La Confiance Numérique : un paysage législatif européen qui s'étoffe

Dès 2010, la Commission européenne a intégré le Marché Unique du Numérique parmi les 7 initiatives phares d'une « stratégie pour une croissance intelligente, durable et inclusive ». C'est dans ce cadre qu'elle publie en 2016 une stratégie pour un marché unique du numérique. En 2020, il est considéré comme un pilier de la reprise suite à la crise de la Covid 19, et de nombreux textes sont élaborés pour permettre la solidification de ce marché unique.

On trouve notamment parmi ces intentions législatives deux textes proposés par la Commission le 15 décembre 2020 : le Digital Markets Act voulant garantir des marchés numériques équitables et ouverts et le Digital Services Act dont l'objectif est de renforcer les règles en matière de responsabilité et de sécurité pour les services numériques et donner un nouveau cadre concurrentiel au marché unique du numérique.

La cybersécurité est devenue pour l'Europe une véritable priorité, la Commission européenne a présenté le 16 décembre 2020 la nouvelle Stratégie de cybersécurité de l'Union européenne à travers laquelle elle veut renforcer la résilience collective de l'Europe face aux cybermenaces tout en permettant aux citoyens et aux entreprises de bénéficier pleinement des services et des outils numériques fiables et dignes de confiance.

Autour de cette stratégie européenne gravitent de nombreux textes relatifs à la confiance numérique dont :

- La révision de la directive NIS (Network and Information Security) proposée par la Commission le 16 décembre 2020 et qui a pour vocation de renforcer la sécurité des systèmes d'information des opérateurs de services essentiels et des fournisseurs de services numériques.
- Le European Cybersecurity Act qui définit clairement des règles communes en matière de certification en cybersécurité au niveau européen. Les premiers schémas de certifications sont en cours et portent sur un Common criteria-based european scheme et sur un cloud computing service. Parmi les schémas de certification futurs on trouve la 5G et les IoTs.
- Le règlement ECCC qui vise à établir un Centre européen de compétence industrielles, technologiques et de recherche en matière de cybersécurité ainsi qu'un réseau de centre nationaux de coordination. Le 9 décembre 2020, le Conseil a décidé que le Centre serait à Bucarest (Roumanie).

Dans le cadre de sa stratégie visant à façonner l'avenir numérique de l'Europe, la Commission soulève également l'importance de l'identité numérique. Dans ce contexte, une révision du règlement e-IDAS est en cours. Ce règlement a pour vocation d'accroitre la confiance dans les transactions électroniques au sein du marché intérieur et faciliter l'émergence d'un marché unique du numérique. Cette révision entraîne des réflexions accrues sur les modalités possibles qui conduiraient à la création d'une identité numérique européenne.

Enfin, l'intelligence artificielle est le dernier sujet majeur dont s'est emparé l'Union européenne afin que cette technologie et ses utilisations soient respectueuses des valeurs et des droits garantis par l'Union. Le 21 avril 2021, la Commission a présenté une proposition de règlement pour l'IA afin de traiter de manière proportionnée les risques liés à des applications spécifiques de l'IA tout en permettant de continuer à la promouvoir et à la développer.

IV) Les tendances de marché

4.8 Les enjeux des grands événements

Corrélé au sujet de la Safe City, la sécurité des grands évènements, qu'ils soient sportifs (JO, mondiaux, etc.), culturels (festivals, grands concerts), diplomatiques (G7, G20, etc.), ou économiques (Salon de l'Auto, Salon du Bourget, MiliPol, Mobile World Congress..), est un thème particulier qui nécessite un ensemble de capacités (contrôle d'accès, gestion des flux, coordination des forces, cybersécurité, détection des menaces, etc.) à mettre en œuvre avec des niveaux de performance élevés sans dégrader l'expérience des participants et si possible en synergie avec d'autres fonctions de l'événement (billetterie, applications, broadcast, etc.) et d'autres fonctions régaliennes ou privées (visa, transport, hôtellerie, etc.).

La filière de sécurité a mené une réflexion afin de déployer une offre française cohérente adaptée à la sécurisation des Jeux Olympiques de 2024 à Paris, et plus largement déclinable à tous types de grands évènements - notamment dans le cadre du CSF (Comité Stratégique de Filière) des Industries de Sécurité.

Ces grands évènements constituent des cibles alléchantes pour les actes malveillants et criminels et notamment les plus graves -tels des actes terroristes ou des cyberattaques- ce qui engendre une menace forte et très évolutive.

Assurer la sécurité des JO est donc un enjeu essentiel avec trois objectifs majeurs : empêcher les attaques et les incidents, détecter les troubles fêtes, et réduire les perturbations au minimum pour les résidents. Mais cette mission combine de nombreuses contraintes : durée de la période à couvrir, sites très nombreux (également au-delà des sites olympiques : fan zones, transports, etc.), public et flux très importants, transparence pour laisser la place à la fête…

La filière de la confiance numérique dispose de fortes compétences, d'une excellence reconnue et de solutions innovantes pour apporter, aujourd'hui et à l'avenir, une réponse évolutive et de très haut niveau aux besoins de sécurité et de confiance numérique des grands évènements. L'objectif du projet est de s'appuyer sur les JO pour valoriser la filière française des industries de sécurité, structurer son offre en matière de sécurité des grands évènements, mettre en avant sa capacité à mettre en œuvre des innovations marquantes et faire progresser les usages et cadres d'emploi des technologies.

A cet égard, les Jeux Olympiques représentent un évènement sportif et de société mondial hors norme, d'une visibilité et d'un impact inégalés qui s'étendront sur une durée bien au-delà de celle -limitée- des jeux eux-mêmes. Réussir les JO sur tous les plans en tant que nation hôte est donc à la fois un impératif et une opportunité exceptionnelle de valoriser le savoir-faire et la marque France, ainsi que de doter le pays d'infrastructures modernisées et sécurisées qui en augmenteront l'attractivité au-delà même de l'héritage olympique.

Il s'agit donc d'une opportunité exceptionnelle pour les entreprises françaises de la confiance numérique de démontrer leur capacité à répondre à un tel défi et de se positionner sur des marchés durables tant au plan national qu'à l'export pour les années à venir.

4.9 Le enjeux de la sécurisation des IoT

La sécurité des objets connectés est répartie sur quatre segments de la Confiance Numérique, correspondant à quatre types de produits :

- *Segment 1.2.1.2 : Identification & Authentification / Segment 2.0.3 : Sécurité des données*
  - *Secure Elements : MCU & CPU sécurisés, systèmes à la fois hard et soft dédié à la protection de données spécifiques particulièrement sensibles (Gemalto, Idemia Starchip, STMicroelectronics)*
- *Segment 2.0.4 : Sécurité des applications*
  - *Le Secureboot, c'est-à-dire le logiciel de sécurisation du programme d'amorçage*
  - *Des semi-conducteurs: processeurs et microcontrôleurs avec des fondations de sécurité nécessaires à la confiance de l'exécution des logiciels (STMicroelectronics)*
  - *Les systèmes d'exploitation de sécurité (tels que le ProvenCore, de Prove and Run), dédiés à la sécurisation des systèmes d'exploitation*
  - *Les hyperviseurs, dédiés à la sécurisation d'un réseau (serveur partagé ou réseau d'objets connectés)*

IV) Les tendances de marché

- *Segment 2.0.5 : Sécurité des infrastructures numériques*
  - La mise à jour du firmware
  - L'authentification, c'est-à-dire la séquence d'authentification machine-to-machine

Les acteurs de la filière considèrent plus l'Internet des Objets comme un nouveau marché que comme une nouvelle technologie. En effet, les solutions conçues pour sécuriser les objets connectés sont dans une large mesure les mêmes que les solutions utilisées pour sécuriser les systèmes informatiques classiques. En conséquence, la sécurisation des objets connectés ne nécessite pas de bouleversement dans la façon qu'ont les entreprises de cybersécurité de concevoir leurs solutions et leurs offres. Seule une adaptation à la marge des solutions existantes est nécessaire.

En revanche, **la sécurisation des objets connectés représente un marché potentiel gigantesque, donc de grandes perspectives de croissances**. Les enjeux de sécurisation des objets connectés ont commencé à être anticipés par les acteurs depuis 2012. En conséquence, la plupart des entreprises de cybersécurité ont déjà préparé des offres dédiées aux objets connectés. Cependant, la croissance annoncée des objets connectés tarde à se faire ressentir si bien qu'en 2019 le marché de la sécurisation des objets connectés était encore de taille modeste.

L'émergence du marché de la sécurisation des objets connectés connait deux freins majeurs :

- Le premier est l'insuffisante standardisation technique des architectures des IoT. Si les clients potentiels mettent en place des réseaux d'IoT qui utilisent tous des objets différents avec une architecture propre, celai rend difficile l'application simple et immédiate des protocoles des fournisseurs des produits cyber sur ces objets. En 2019, l'initiative de l'ETSI (European Telecommunications Standard Institute) de publier des spécifications techniques de base pour l'IoT a constitué une véritable avancée (voir le communiqué de l'ACN sur ce sujet), malheureusement encore insuffisante car pour certains objets connectés pouvant être utilisés dans des applications nécessitant un grand niveau d'assurance, il est impératif de compléter ces règles minimales par des procédures plus robustes en termes d'exigences de cybersécurité.

- Le second frein est l'axe de développement actuel des objets connectés. Il semble en effet que les plateformes IoT existantes pour le moment portent plus sur des projets BtoB que sur des projets BtoC. Or, 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 sécurisation de 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. La sécurisation des objets connectés BtoC -qui sont souvent des objets isolés mais en interaction sur des réseaux de grandes tailles- nécessite au contraire nécessairement l'élaboration de solutions nouvelles dédiées et représentent donc un potentiel de croissance supérieur aussi bien en volume qu'en valeur. La sécurisation de la voiture connectée a été le principal moteur de la croissance de ce segment sur la période 2013-2018 (avec une croissance de 7% à 10% par an), mais la chute de la croissance du marché automobile mondial à partir de 2017 (principalement dû au ralentissement du marché chinois) puis la crise de la COVID-19 en 2020 ont freiné cette croissance depuis 2018. Parmi les principaux acteurs dans ce domaine, on trouve Thales Digital Identity and Security, Idemia, Cap Gemini, Telit, Sierra wireless, etc.

Les plateformes IoT sont en revanche l'opportunité de l'émergence d'un nouveau business model au forfait : intégrer des puces dans divers objets connectés, facturer ces puces à la vente, puis facturer un forfait d'usage de ces puces une fois les réseaux d'objets connectés installés.

Enfin, en matière d'ingénierie et de R&D, **la France est dans la moyenne haute mondiale dans ce domaine**. Il s'agit de la thématique sur laquelle le groupe cybersécurité de l'Allistene (Alliance des sciences et des technologies du numérique), a le plus axé ses efforts depuis 2017.

Pour transformer ce marché potentiel, il est primordial que le secteur de la Confiance Numérique capitalise sur les outils de certification mis en place par le European Cybersecurity Act et mène une action collective pour élaborer et proposer un référentiel de cyber-sécurisation des IoT à l'usage des secteurs utilisateurs, à l'instar des travaux d'ores-et-déjà menés par Eurosmart.

IV) Les tendances de marché

4.10 Matrice FFOM de la Confiance Numérique en France

Forces	Faiblesses
Structures • Des grands groupes et des spécialistes efficaces, avec de fortes positions internationales. • Un système de promotion de l'innovation et de la recherche performant (CIR, etc.). • Des structures fédératrices : ACN, le CSF Industries de Sécurité, les Pôles de compétitivité (SYSTEMATIC, SAFE, SCS, Pôle d'excellence cyber, Bretagne Développement Innovation, Cap Digital, TES, Images et réseaux, etc.), l'INRIA, etc. • La spécificité française en matière de protection des données individuelles à travers les actions menées par la CNIL permet de maintenir un avantage compétitif des acteurs français vis-à-vis des acteurs étrangers, notamment en matière de web filtrage. En effet, les entreprises françaises construisent des offres dédiées à la réglementation française, tandis que les grands concurrents internationaux développent des offres standardisées à l'échelle mondiale qui ne correspondent pas complètement à la réglementation française. • Une résilience à la crise du COVID portée par une demande structurelle forte en biens et services de Confiance Numérique. **Compétences** • Capacités techniques et de R&D de premier rang mondial. • Fort leadership de compétences dans de nombreux domaines (identification & authentification, gestion de l'identité, cryptographie, machine learning, deep learning, sécurisation des IoT et dans une moindre mesure blockchain). • Une filière de formation forte pour les compétences d'ingénierie et de développement logiciel avec la création de chaires cybersécurité en partenariat publics-privés. • Capacités fortes d'innovation et d'initiative.	**Structures** Les PME françaises de cybersécurité sont chacune spécialisées dans un sous-segment spécifique et ne proposent que des offres sur-mesure. En conséquence, les PME de cybersécurité françaises travaillent très majoritairement avec des grands comptes (CAC40 et grandes ETI). Une solution pour qu'elles développent leur clientèle de PME françaises et internationales consiste à développer des partenariats entres les PME françaises de la cybersécurité (pour proposer des offres communes, mettre en commun des compétences ou des opportunités d'exportation…). Sans cela, elles seront cantonnées dans des offres haut de gamme et sur-mesure auprès de quelques grandes entreprises et administrations. **Compétences** • On observe -à l'exclusion des quelques géants français- un rapport de 1 à 10 entre les effectifs dédiés à la R&D au sein des entreprises françaises de cybersécurité et leurs concurrents américains. • Bien que la France ne souffre pas de retard en matière de formation à la cybersécurité, la croissance est telle dans ce secteur que les compétences sont difficiles à trouver. Les premières embauches de développeurs spécialisés dans un domaine spécifique de la cybersécurité (PKI, cryptographie, etc.) est quasiment impossible. Les entreprises sont contraintes d'embaucher dans le meilleur des cas des développeurs formés à la cybersécurité dans son ensemble, voir des ingénieurs généralistes qui seront formés en interne. **Attitudes** • Chasse en meute encore peu développée. • PME souvent attaquées sur le marché français, rachetées et/ou désarmées à l'international. • Les prescriptions des pouvoirs publics (notamment de l'ANSSI), sont insuffisamment mises en œuvre, notamment par les OIV. Les offreurs français de solutions de cybersécurité souffrent de cette situation.

Opportunités

Structures

- La confiance numérique est parmi les filières industrielles qui croissent le plus en France et dans le monde avec un taux moyen de plus de 8% par an sur la période 2015-2020.
- Combiner une commande publique forte et le triptyque standardisation-certification-prescription pour favoriser l'accession des entreprises françaises à des marchés à volumes importants, leur permettant d'atteindre la taille critique nécessaire dans l'économie actuelle globalisée.
- Structuration croissante de l'offre dédiée « sécurité » des entreprises et des équipes dédiées « sécurité » chez les clients.
- Mise en oeuvre du RGPD.
- Certification sécuritaire des objets IoT (CyberSecurity ACT).

Attitudes

- Suite aux évènements récents: affaire Snowden, American Cloud Act, crise du COVID-19, etc. augmentation de la prise de conscience de la nécessité d'une souveraineté au niveau de la confiance numérique, non seulement pour les services publics et les OIV mais également pour les citoyens et la défense commerciale des entreprises françaises.
- En raison de la diversité des PME françaises en matière de cybersécurité, les entreprises françaises ont des offres souvent moins lisibles et plus difficilement comprises par la clientèle, en particulier en comparaison des offres américaine. Ce manque de lisibilité provient principalement de l'absence d'une offre française généraliste. La France a donc l'opportunité de travailler à l'élaboration d'offres de cybersécurité globales regroupant les divers acteurs de la filière tout en s'inspirant des stratégies marketing américaines.

Nouvelles technologies / offres en croissance

- Développements cryptographiques: cryptographie légère, cryptographie quantique et post-quantique, chiffrement homomorphique, cryptographie utilisant l'ADN ou encore des réseaux de neurones antagonistes génératifs…
- Innovations en matière d'éléments sécurisés : embarqués, intégrés, soft secure elements type Trusted Execution Environment (TEE), etc.
- Intelligence Artificielle : biométrie comportementale, etc.
- Blockchain.
- Plateformes d'open hardware/software pour l'edge computing et les IoTs.
- Innovations relatives à l'identité numérique.
- Analyse en temps réel des données d'observation large zone.

Nouveaux marchés / marchés en croissance

- Sécurisation des objets connectés: automobile, safe city…
- Thématique de la souveraineté des données.
- Identité numérique.
- La plupart des marchés de la cybersécurité…

Menaces

Structures

- Développement de standards américains ou autres sur les nouveaux marchés.

Compétences

- Fuite des talents, en particulier en matière de deep learning. Les entreprises françaises (en particulier les PME), ont du mal à s'aligner sur les salaires offerts par les grands acteurs américains qui proposent en général des salaires supérieurs de 10% à 30% à compétences égales.

Concurrence

- Concurrence américaine et chinoise s'appuyant sur de très grands marchés nationaux et des politiques publiques volontaristes. Avec une intensité bien moindre, concurrence en provenance d'Allemagne, de Grande Bretagne, du Japon, d'Israël, et de Suède.
- Entreprises US puissantes (finance, marketing, R&D, réseau international et réseau de partenaires) tout particulièrement dans la partie Cybersécurité ou les généralistes de l'IT se renforcent.
  - En matière de services de cybersécurité, les grands cabinets américains d'audit et de conseil disposent de surfaces financières inégalables pour leurs concurrents européens (à l'exception de Thales, Atos, Capgemini et Orange Cyberdéfense) et ont des stratégies agressives de rachat d'entreprises françaises innovantes et de pression à la baisse sur les prix.
  - Les GAFA continuent d'accroître leurs parts de marché en matière de sécurité, en particulier en matière d'IAM (Identity Access Management), où la France est leader. Ces GAFA ont la volonté d'imposer des solutions « tout numérique », c'est-à-dire sans composante hardware, générant à coup sûr des failles de sécurité des utilisateurs vis-à-vis de ces mêmes GAFA.
- Montée en gamme des entreprises asiatiques et en premier lieu chinoises, particulièrement en matière de produits cyber.
- Acquisition significative d'entreprises françaises par des capitaux américains sur la période 2016-2021.

Attitudes

- Prise de conscience encore trop faible des nouveaux clients de l'importance des enjeux de sécurité et surtout de Sécurité by Design, en particulier dans le domaine des objets connectés qui comporte de nombreux nouveaux entrants non issus des filières industrielles plus familières de ces enjeux (électronique, défense, etc.).

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 la cybersécurité, de l'identité numérique, des communications sécurisées, de la traçabilité / lutte anti-contrefaçon et de la Safe City. 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 près de 2 100 entreprises réalisant en France 13,4 Milliards d'euros de chiffre d'affaires dans ce secteur en forte croissance (8,1% de croissance annuelle moyenne depuis 2015).

Les membres de l'Alliance pour la Confiance Numérique (ACN), dont 75% de PME/TPE-ETI, représentent 65% 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) 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*).

Liste des membres

Partenaires

A propos de DECISION Etudes & Conseil

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, des organisations professionnelles ou des institutions financières et des fonds d'investissements, mais également les pouvoirs publics locaux et nationaux (gouvernements, ministères, etc.) ainsi que la Commission Européenne.

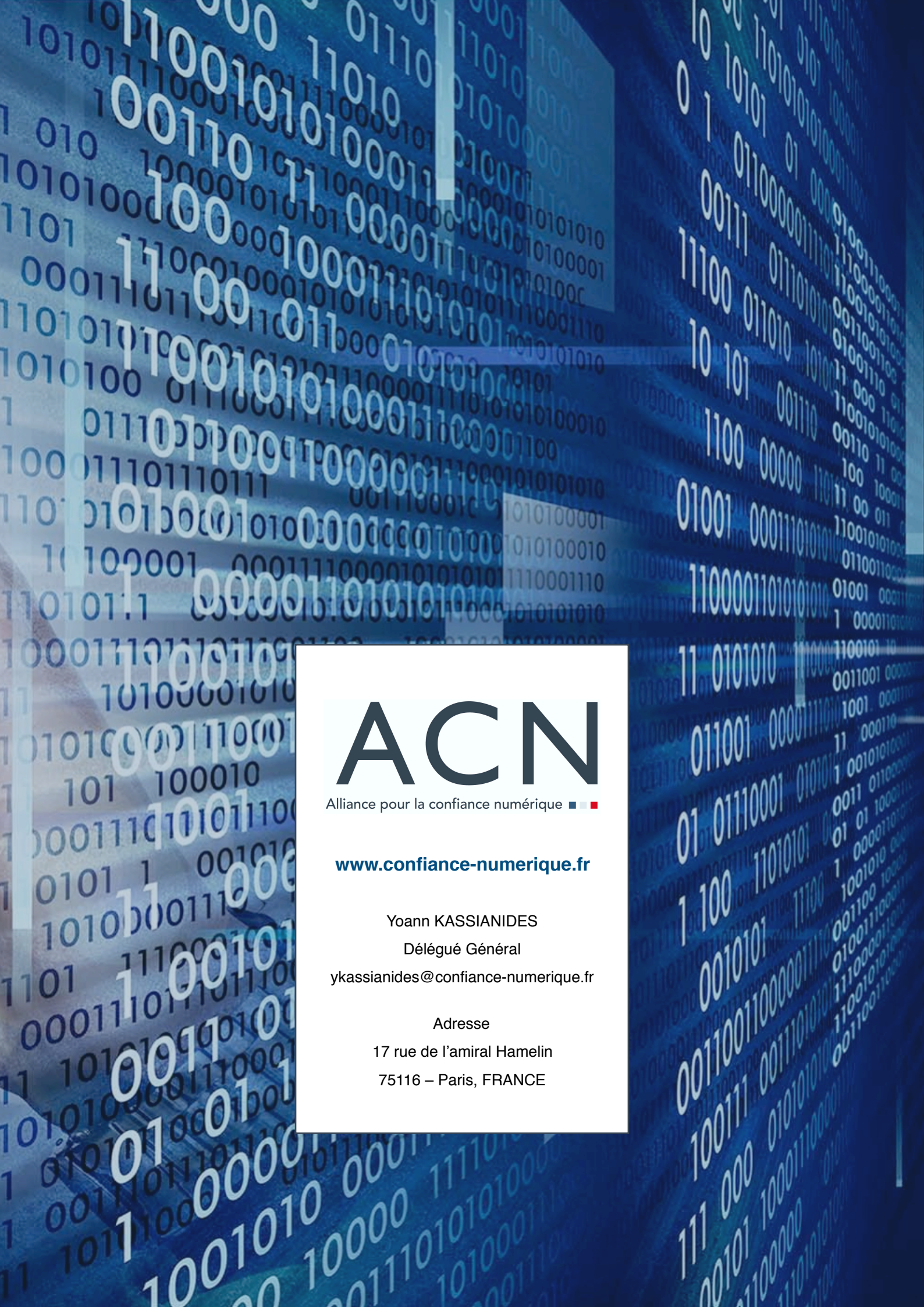
En 2009, DECISION initie et conduit la première étude pour la Commission Européenne sur l'industrie de sécurité et est un des partenaires du contrat-cadre (2010-2015) sur l'industrie de sécurité (incluant la cybersécurité) pour la DG ENTR de la Commission Européenne.

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.

Pour plus d'informations :
www.decision.eu

DECISION
ETUDES & CONSEIL



ACN

Alliance pour la confiance numérique

www.confiance-numerique.fr

Yoann KASSIANIDES

Délégué Général

ykassianides@confiance-numerique.fr

Adresse

17 rue de l'amiral Hamelin

75116 – Paris, FRANCE