L'Observatoire de la filière de la Confiance Numérique

2020

ACN
Alliance pour la Confiance Numérique
www.confiance-numerique.fr

Le mot du Président

Chaque année depuis bientôt dix ans, l'Alliance pour la Confiance Numérique (ACN) recense et rend publiques les principales données économiques du domaine de la confiance numérique dont elle assure la représentation institutionnelle, compris comme l'ensemble des entreprises qui contribuent à sécuriser le numérique et à permettre son utilisation en toute confiance (principalement les secteurs de l'identité numérique, de la cybersécurité et du numérique de confiance).

Au regard des éditions successives de l'Observatoire ACN de la confiance numérique, trois caractéristiques apparaissent avec force : **le dynamisme du taux de croissance annuel** qui oscille chaque année autour de 10%, l'apport de ce secteur au reste de l'économie **avec un taux de valeur ajoutée supérieur à tous les autres domaines**, ainsi que **la qualité du 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.

L'édition 2020 de l'Observatoire ne dément pas ces grandes orientations. Pour l'année 2019, scannée par cet Observatoire, les quelque 2000 entreprises de la confiance numérique employaient 67 000 salariés et représentaient 13 milliards d'euros de chiffre d'affaires (en hausse de 8,8% par rapport à l'année précédente).

Cette édition portant sur l'année 2019 ne prend pas en compte les effets de la pandémie mondiale. Un baromètre ACN-Covid19 a été mis en place pour mesurer l'impact de cette crise dans le secteur. Il apparait que les entreprises de la confiance numérique sont diversement affectées mais une lecture d'ensemble de ces réponses permet d'anticiper **un impact globalement limité sur les dynamiques du secteur à court terme**.

A moyen terme et en sortie de crise**, le secteur de la confiance numérique présente de nombreux atouts pour devenir un des fers de lance de la relance économique**. En effet, les mesures de confinement édictées pour lutter contre la pandémie ont démontré **le caractère stratégique et vital de l'ensemble des usages numériques** pour faire fonctionner l'économie et plus largement la société, mais aussi **notre dépendance à des outils, services des infrastructures de pays tiers**. **La souveraineté numérique nationale et l'autonomie stratégique européenne sont, dans ce nouveau contexte, des enjeux cruciaux auxquels le domaine de la confiance numérique apporte des réponses efficaces** compte tenu de ses caractéristiques et de ces atouts intrinsèques.

Aussi, **faisons de cette crise une opportunité historique de conforter l'essor d'une industrie de la confiance numérique souveraine et de premier ordre**, qui permettra d'adresser simultanément les défis stratégiques, économiques et sociaux que la crise du Covid19 a mis en évidence. La confiance numérique est le facteur déterminant pour que notre pays ressorte de cette épreuve grandi et se mette en mesure de maitriser son avenir numérique.

Philippe Vannier

Président de l'ACN, Atos

Sommaire

Etude définie et commanditée par l'**Alliance pour la Confiance Numérique (ACN)**

Alliance pour la Confiance Numérique

11-17 rue de l'amiral Hamelin
75116 Paris

www.confiance-numerique.fr - contact : ykassianides@confiance-numerique.fr

Etude réalisée par **DECISION Etudes & Conseil**

DECISION
ETUDES & CONSEIL

www.decision.eu

Éléments clefs

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

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

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

L'ACN a mis en place un **Observatoire de la Confiance Numérique** pour recueillir et mettre en commun des données sur les grandes caractéristiques et les tendances de cette filière ; c'est dans ce cadre que cette étude a été réalisée en 2020, couvrant le champ de la cybersécurité et de la sécurité numérique.

La Confiance Numérique en France en 2019 c'est :

- **13 milliards d'euros de chiffre d'affaires**, soit 8,8% de croissance entre 2018 et 2019
- **6,1 milliards d'euros de valeur ajoutée**
- **67 000 personnes employées** dans le secteur
- Un **chiffre d'affaires** réparti à **57% pour la Cybersécurité et à 43% pour la Sécurité Numérique**

Les entreprises françaises de la Confiance Numérique dans le Monde en 2019 c'est :

- **21 milliards d'euros de chiffre d'affaires** générés dans le Monde par la filière française de la Confiance Numérique *(CA France, CA exporté depuis la France et CA réalisé à l'étranger par des entreprises détenues par des capitaux français)*
- Des **leaders mondiaux** sur les segments de la sécurité numérique (Thales, Airbus 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).
- **12,4 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)
- **4,4 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 :

- **8,8%** de croissance moyenne annuelle en France sur la période 2014-2019, contre **1,5%** pour le PIB français
- La Confiance Numérique est la **filière industrielle française qui bénéficie de la croissance la plus forte**
- **La croissance de la Confiance Numérique est stable depuis 10 ans et devrait se maintenir sur la période 2019-2024 grâce notamment aux IoT, à l'automobile connectée, à la 5G, à la transformation digitale, à la Safe City, etc.**
- 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 :

- **2 134 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 **1 355 micro-entreprises**, générant moins de 2 millions de CA en 2019

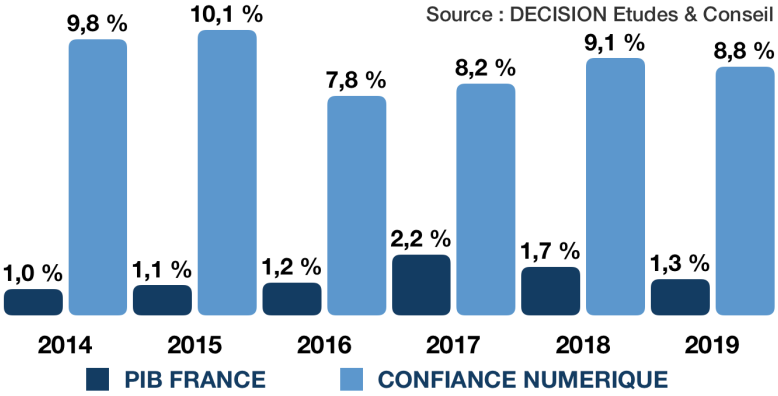
Éléments clefs

FONDAMENTAUX 2019

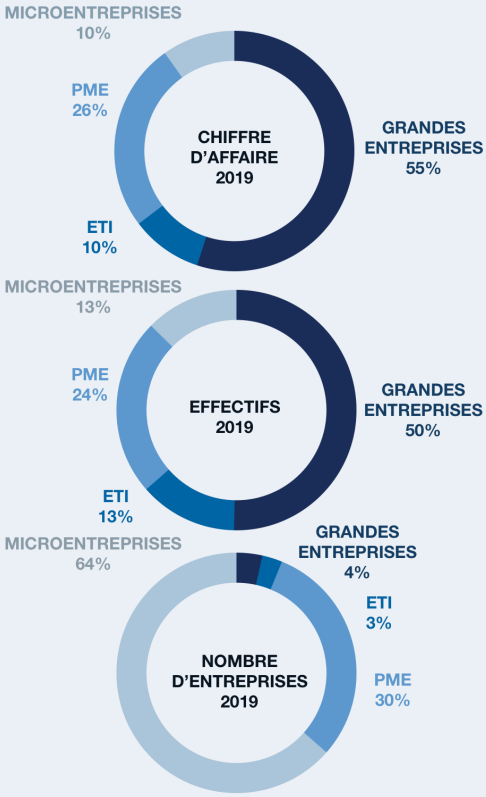
CA MONDE	21 MDS €	CROISSANCE 2018-2019
CA HORS DE FRANCE	8 MDS €	8,8%
CA FRANCE	13 MDS €	
DONT CA EXPORT	4,4 MDS €	65 700 EMPLOIS EN FRANCE
VA FRANCE	6,1 MDS €	
MARCHÉ FRANÇAIS	11,4 MDS €	

Source : DECISION Etudes & Conseil

CROISSANCES COMPARÉES 2014-2019

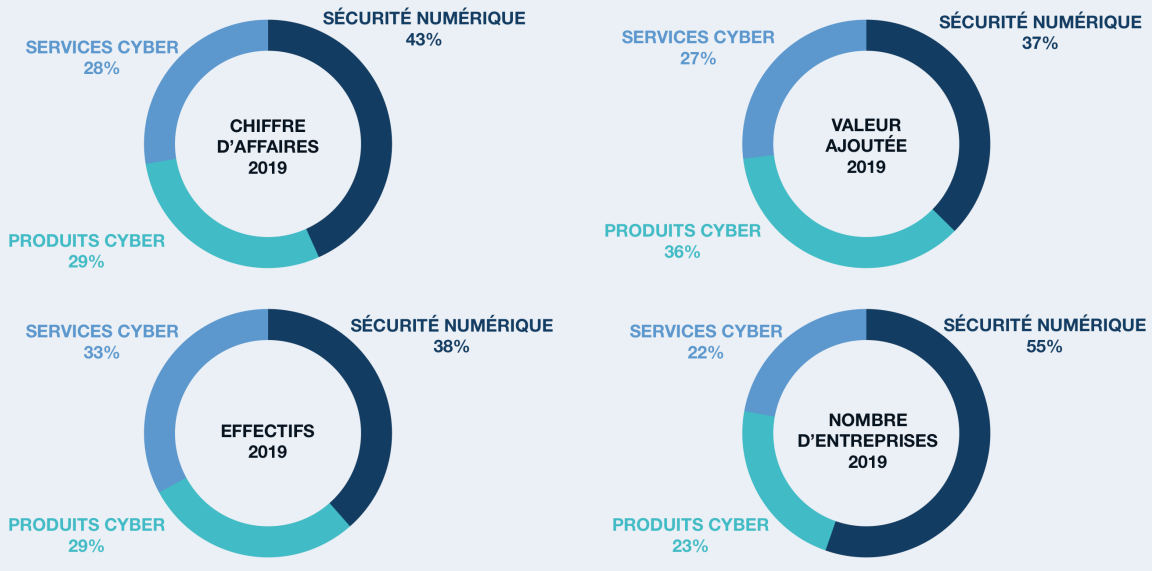


ANALYSE PAR TAILLE D'ENTREPRISES



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 clefs

TOP 10 ACTEURS FRANCE- 2019

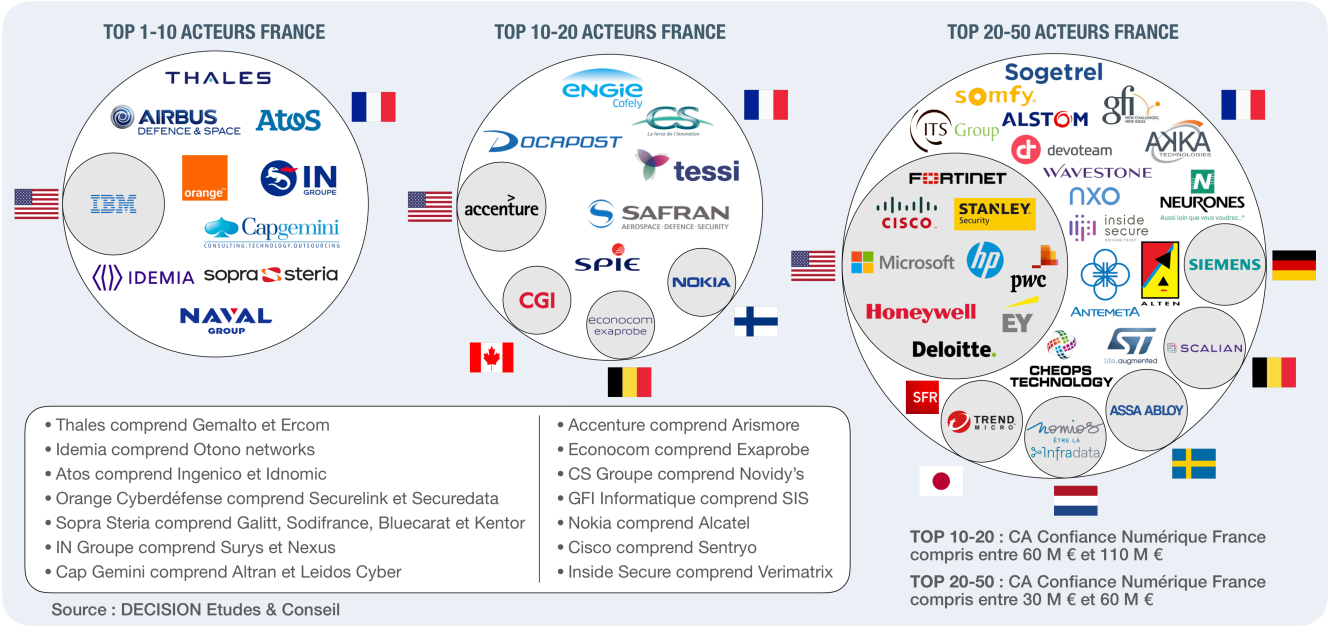
N°	ENTREPRISE	CA CONFIANCE NUMÉRIQUE FRANCE	CA CONFIANCE NUMÉRIQUE MONDE	N° MONDE
1	THALES	1 541 M €	4 597 M €	1
2	IDEMIA	1 012 M €	2 112 M €	3
3	ATOS	503 M €	1 012 M €	5
4	AIRBUS D&S	491 M €	808 M €	6
5	IBM	298 M €	2 348 M €	2
6	IN GROUPE	278 M €	456 M €	9
7	ORANGE CYBERDEFENSE	272 M €	676 M €	7
8	CAP GEMINI	230 M €	1 127 M €	4
9	SOPRA STERIA	200 M €	497 M €	8
10	NAVAL GROUP	123 M €	123 M €	10

Source : DECISION Etudes & Conseil

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

- **Thales** crée un leader mondial de la sécurité digitale avec le rachat de Gemalto ;
- **Thales** et **Idemia** sont des leaders mondiaux 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 Storia** sont les 5 leaders français parmi les entreprises de services du numérique (classement teknowlogy / PAC), et sont également les leaders français en cybersécurité (avec Thales et Airbus D&S) ;
- **IN Groupe** (ex Imprimerie Nationale) est un leader de l'identité numérique européen ;
- **Worldline** est également un leader mondial de la sécurisation des paiements. Worldline s'est séparé d'Atos début 2020.

Si les 9 premières entreprises de la filière ont des activités nettement plus importantes que les autres en France avec un CA de plus de 200 M€ chacune, les six entreprises situées entre la dixième position et la quinzième position sont en revanche très proches avec un CA France compris entre 94 M€ et 123 M€. Il s'agit des français Naval Group, SAFRAN, Tessi et Groupe CS ainsi que de l'américain Accenture et du belge Econocom. De même, 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.



- Thales comprend Gemalto et Ercom
- Idemia comprend Otono networks
- Atos comprend Ingenico et Idnomic
- Orange Cyberdéfense comprend Securelink et Securedata
- Sopra Steria comprend Galitt, Sodifrance, Bluecarat et Kentor
- IN Groupe comprend Surys et Nexus
- Cap Gemini comprend Altran et Leidos Cyber
- Accenture comprend Arismore
- Econocom comprend Exaprobe
- CS Groupe comprend Novidy's
- GFI Informatique comprend SIS
- Nokia comprend Alcatel
- Cisco comprend Sentryo
- Inside Secure comprend Verimatrix

Source : DECISION Etudes & Conseil

TOP 10-20 : CA Confiance Numérique France compris entre 60 M € et 110 M €

TOP 20-50 : CA Confiance Numérique France compris entre 30 M € et 60 M €

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 communications numériques, 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, communication, etc.).

L'ACN, au coeur de la Confiance Numérique :

Les adhérents de l'ACN représentent :

- Plus de **70%** du chiffre d'affaires de la Confiance Numérique réalisé par les entreprises françaises dans le monde.
- Près de **60%** du chiffre d'affaires de la Confiance Numérique réalisé par les entreprises françaises en France.
    - **75%** en sécurité numérique.
    - **40%** en cybersécurité.
- **45%** du chiffre d'affaires réalisé en France par l'ensemble de la filière de la Confiance Numérique[1].
    - **60%** en sécurité numérique.
    - **30%** en cybersécurité.

Parmi les adhérents de l'ACN, on trouve 35% de grandes entreprises et 65% d'ETI, de PME et de micro entreprises.

[1] En effet, la filière regroupe des acteurs étrangers importants qui ne sont pas membres de l'ACN, ainsi que de nombreux cabinets de conseil en transformation digitale dont une partie de l'activité consiste en du service de cybersécurité et qui ne font pas partie de l'ACN.

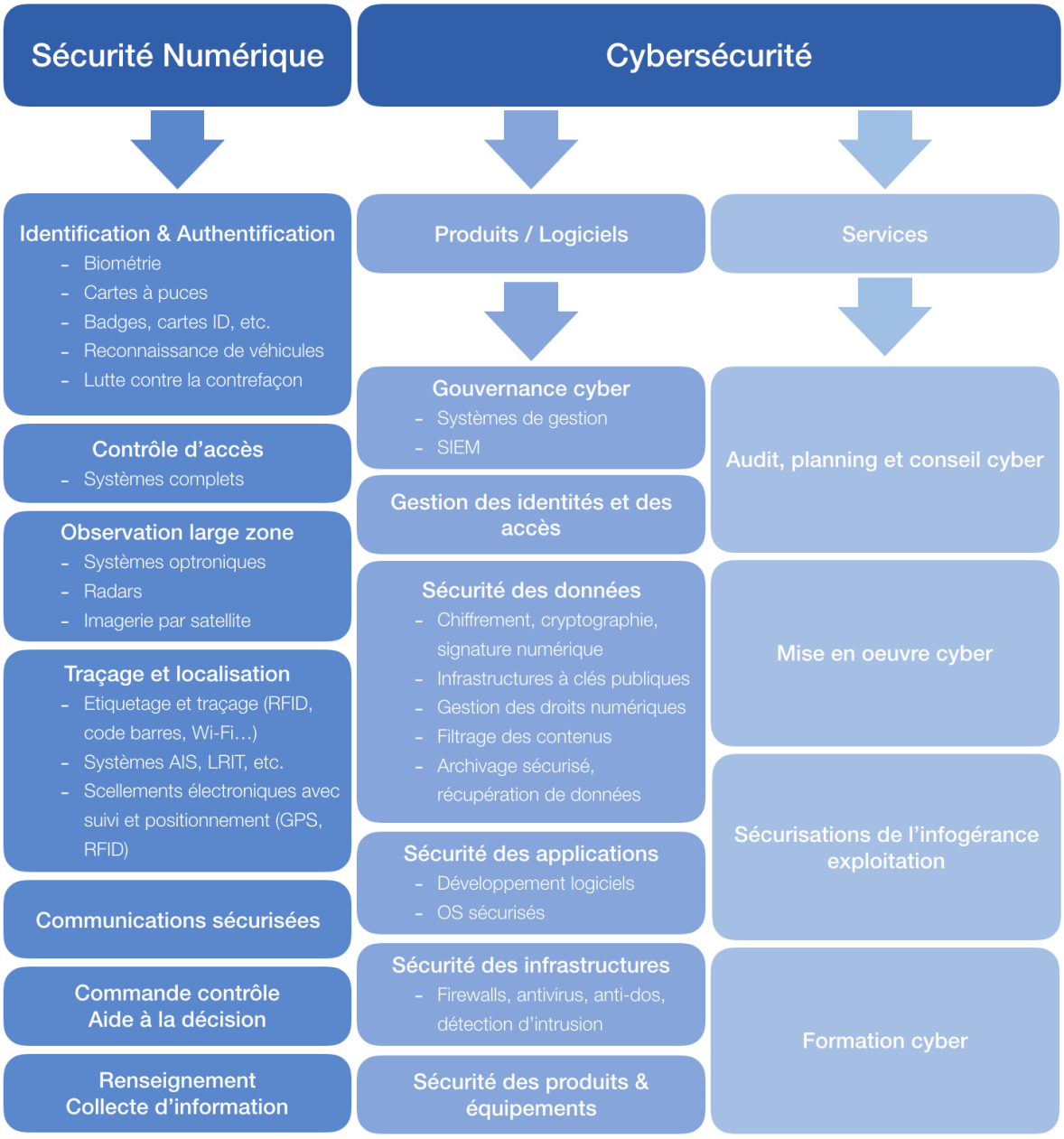
I) Confiance Numérique :
Cybersécurité et Sécurité Numérique

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



I) Confiance Numérique :
Cybersécurité et Sécurité Numérique

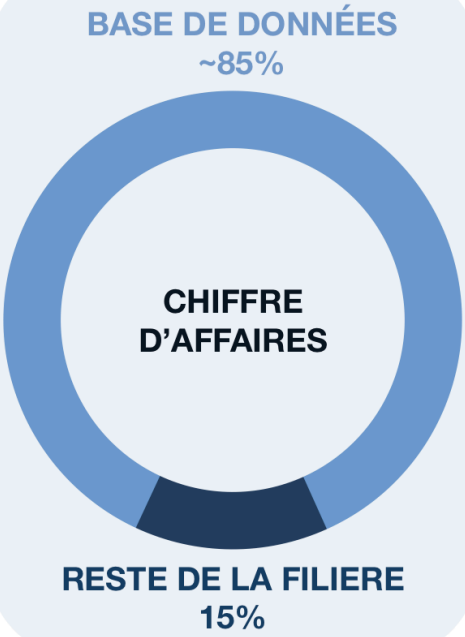
1.3 Méthodologie

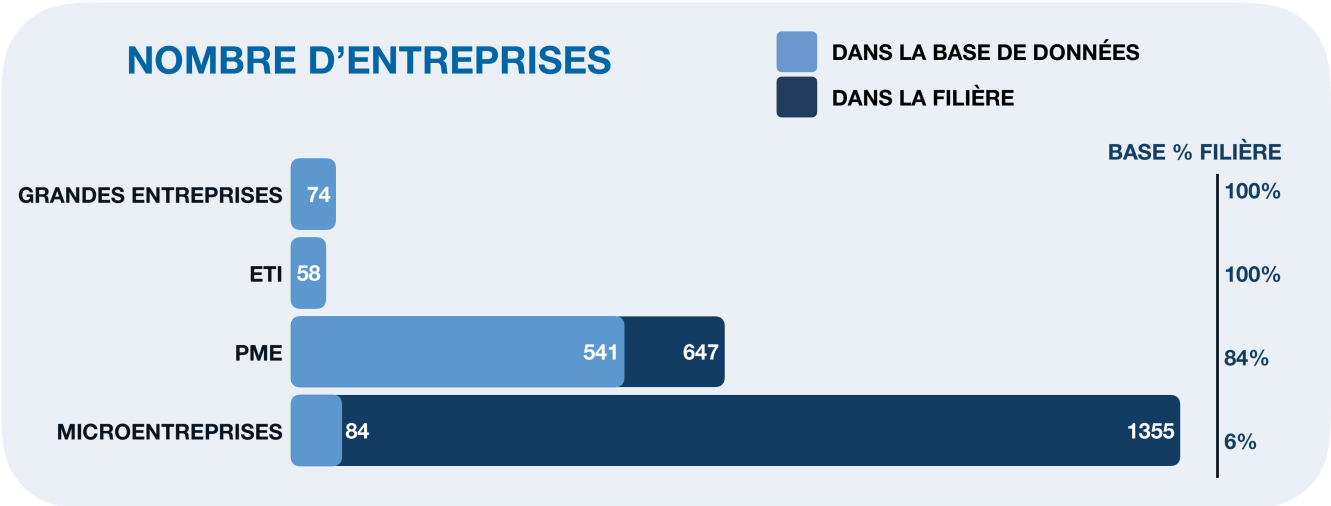
L'objectif de l'Observatoire est à la fois de définir le périmètre de la filière de la Confiance Numérique et d'en évaluer le poids économique et les caractéristiques.

Les données présentées dans ce rapport sont issues d'une base de données 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

Pour chaque entreprise de la base de données ont été collectées 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 2014-2019 : Chiffre d'affaires, effectifs, chiffre d'affaires à l'exportation, valeur ajoutée, résultat net.
- DECISION a ensuite effectué une analyse spécifique à chaque entreprise afin d'estimer la part de l'activité dédiée à la sécurité, et la répartition du chiffre d'affaires selon les 45 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 a été réalisée grâce à l'expertise de DECISION sur le secteur de la sécurité depuis 10 ans.

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.

Une analyse spécifique de l'évolution de l'activité mondiale (globale et sécurité), des principaux acteurs de la Confiance Numérique a été effectuée, permettant d'estimer le chiffre d'affaires réalisé par la filière à l'étranger ainsi que son évolution.

Enfin la croissance par segment a été mesurée directement en collectant lorsque cela était possible l'évolution des activités des principaux acteurs (grands groupes et grandes ETI), sur les segments concernés en France. Pour le reste de la filière, une analyse en sous-échantillon a été 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 des activités sur le segment concerné. Les croissances affichées dans ce rapport sont donc les résultats d'un arbitrage entre trois composantes :

- Les croissances sur le segment concerné en France des principaux acteurs ;
- Les croissances totales en France des acteurs représentatifs de chaque segment (c'est-à-dire dont le CA du segment dépasse 30% du CA total) ;
- Les analyses des acteurs clefs interrogés lors des entretiens directs conduit en 2020, en 2018, en 2017 et en 2015.

Les chiffres sont construits sur l'année 2018 et extrapolés sur l'année 2019.

AMÉLIORATIONS PAR RAPPORT AU PRÉCÉDENT OBSERVATOIRE

Depuis le précédent Observatoire, un travail d'analyse a été effectué sur l'ensemble des grandes entreprises et des entreprises intermédiaires de la filière dans le but de mieux prendre en compte leurs activités de confiance numérique et de mieux les segmenter.

En conséquence de ces améliorations, **les chiffres de l'Observatoire 2020 ne sont pas directement comparables avec ceux de l'Observatoire précédent**. Les chiffres de cet Observatoire sont présentés pour l'année 2019 et en fonction de la nouvelle segmentation des acteurs. Les chiffres 2018 actualisés sont présentés page 13 de ce rapport.

II) Confiance Numérique :

Une filière importante et dynamique

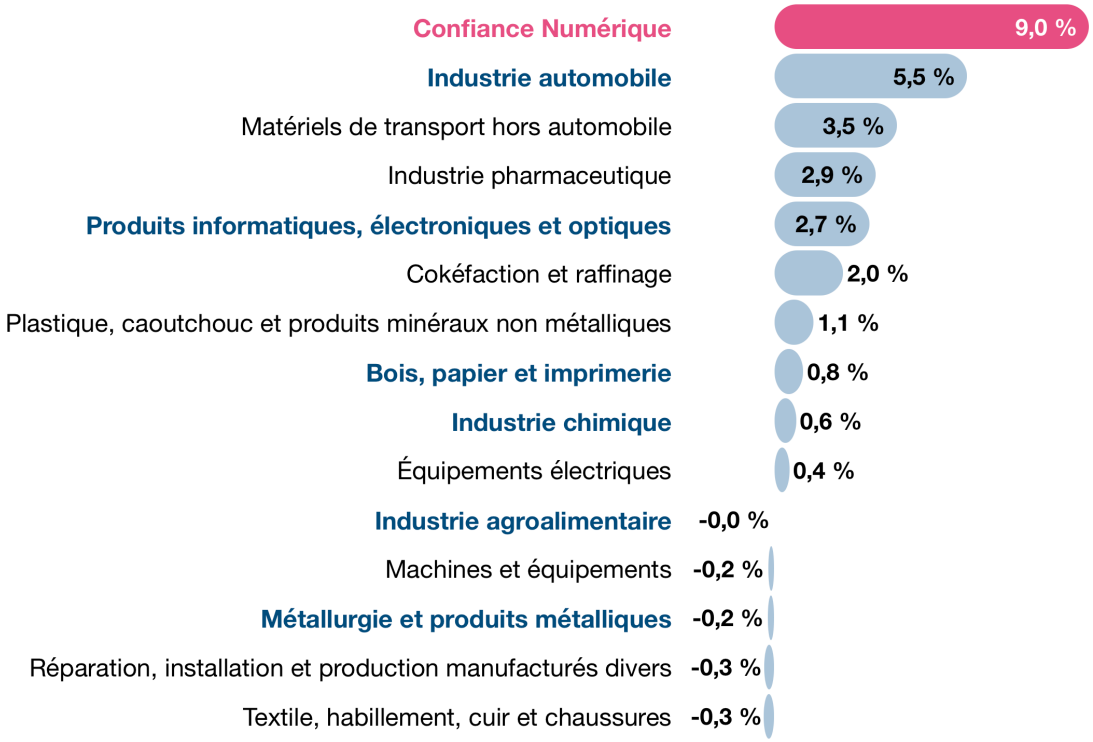
2.1 La Confiance Numérique est l'industrie française qui bénéficie de la croissance la plus forte

Sur la période 2014-2019, la Confiance Numérique est de loin la filière industrielle avec le plus fort taux de croissance avec 9%/an. De tels niveaux de croissance ne se retrouvent dans aucune autre branche de l'industrie manufacturière française.

Si bien qu'à horizon 2025, la Confiance Numérique devrait devenir la 12ème filière industrielle française sur 15 en valeur ajoutée en dépassant la filière des équipements électriques.

A horizon 2030, la filière de la Confiance Numérique devrait dépasser la filière de « Bois, papier et imprimerie » et pourrait également rattraper et dépasser les filières des « Produits informatiques, électroniques et optiques » et des « Machines et équipements ».

CROISSANCE ANNUELLE MOYENNE DES FILIÈRES FRANÇAISES SUR LA PÉRIODE 2014-2019



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

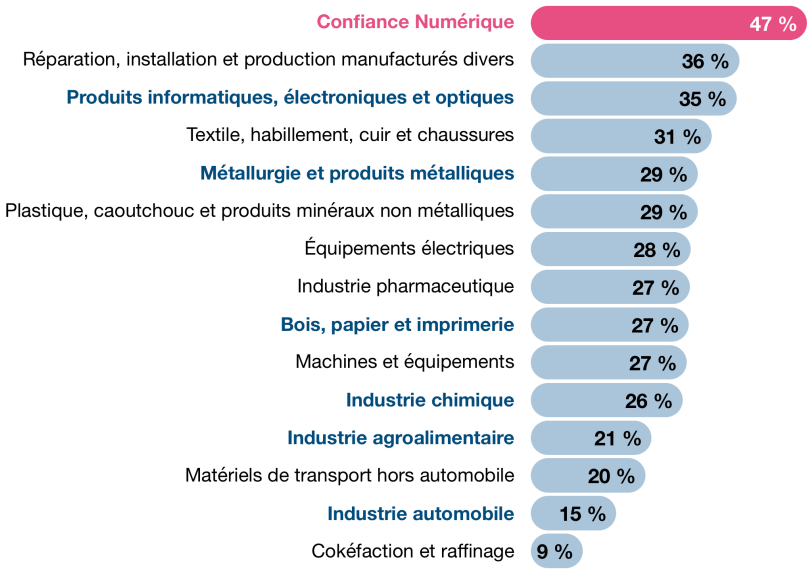
2.2 La Confiance Numérique est la filière industrielle dont l'activité est la plus créatrice de richesse en France

La Confiance Numérique est de loin 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 :

- Le pourcentage de l'activité dédiée aux services est relativement élevé dans l'industrie française de Confiance Numérique, à travers les services de cybersécurité (conseil, audit, formation, etc. qui ont représenté 28% du CA total en 2018). 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. Les deux autres phénomènes décrits ci-dessous sont les vraies causes de ce que l'industrie de sécurité occupe la première place.
- Les produits électroniques dédiés à la Confiance Numérique (sécurité numérique) correspondent à 43% du chiffre d'affaires total de la filière de Confiance Numérique, soit près de la moitié. 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.
- Enfin, les produits de cybersécurité correspondent à 29% du CA total de la filière de sécurité en 2018 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 2019



Sources : DECISION, Eurostat, OCDE

Bleu = Industries qui disposent à la fois d'un segment Eurostat dédié et d'un CSF auprès du CNI

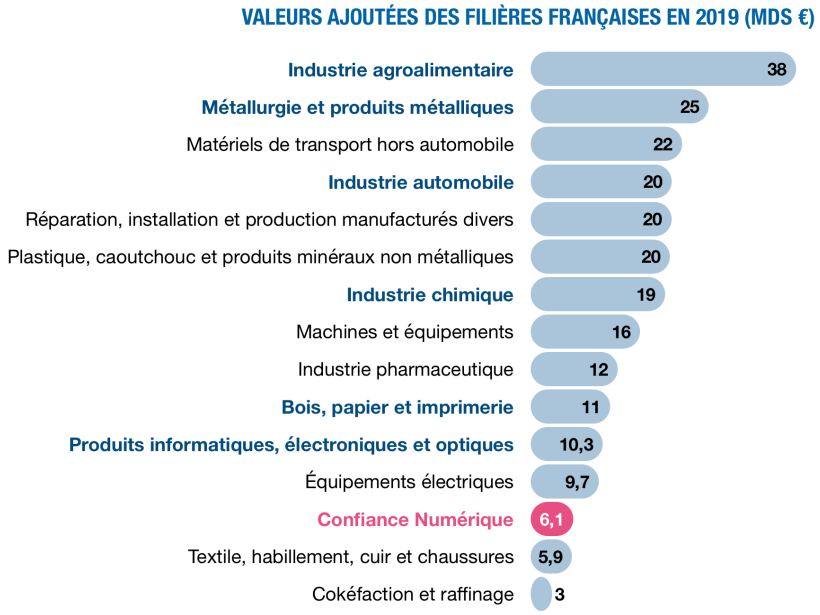
Noir = Industries segmentées par Eurostat et qui correspondent plus ou moins à des filières disposant d'un CSF auprès du CNI (à voir au cas par cas)

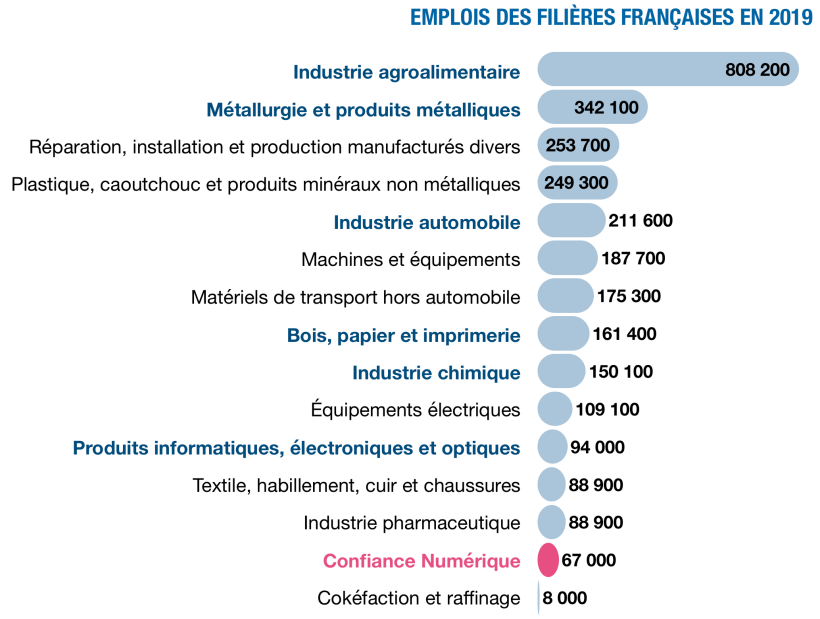
II) Confiance Numérique :

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 de Textile, habillement, cuir et chaussures 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 pharmaceutique.





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 à Paris 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**. Les entreprises et administrations du monde entier digitalisent leurs processus et interconnectent les réseaux de données ainsi générés. Ce phénomène 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…

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 78% du chiffre d'affaires de la Confiance Numérique en France, soit 10 milliards d'euros en 2019. Autrement dit, les acteurs étrangers de la filière réalisent 22% du chiffre d'affaires de la filière en France, soit environ 2,8 milliards d'euros en 2019. 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 peut paraître encore assez élevée, elle baisse régulièrement depuis 2013 et devrait continuer à baisser sur la période 2019-2024. Les entretiens directs que DECISION conduit régulièrement avec les acteurs clefs de la filière indiquent la présence de plus en plus forte d'acteurs étrangers, principalement américains et dans une moindre mesure chinois.

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 2013-2019. 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.

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 sur la période 2013-2019. En effet, dans un contexte général de stagnation de la croissance (1,4%/an de croissance du PIB français sur la période 2013-2019), 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 prix mais également sur 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 donc une filière dont le caractère stratégique doit être désormais reconnu, 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.

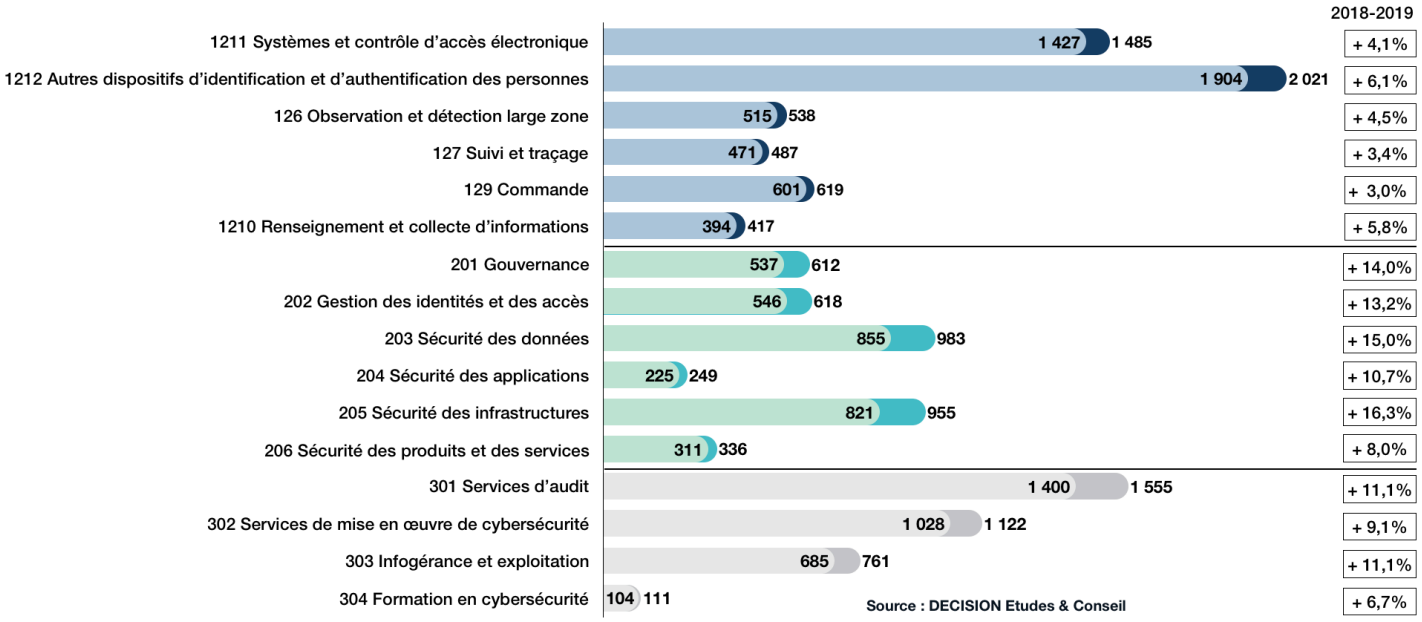
Les conditions sont réunies pour que l'effet de levier en cas de mise en place d'une politique industrielle volontariste génère un maximum de retour sur investissement, aussi bien en termes d'emploi que de valeur ajoutée sur le sol français et à l'international.

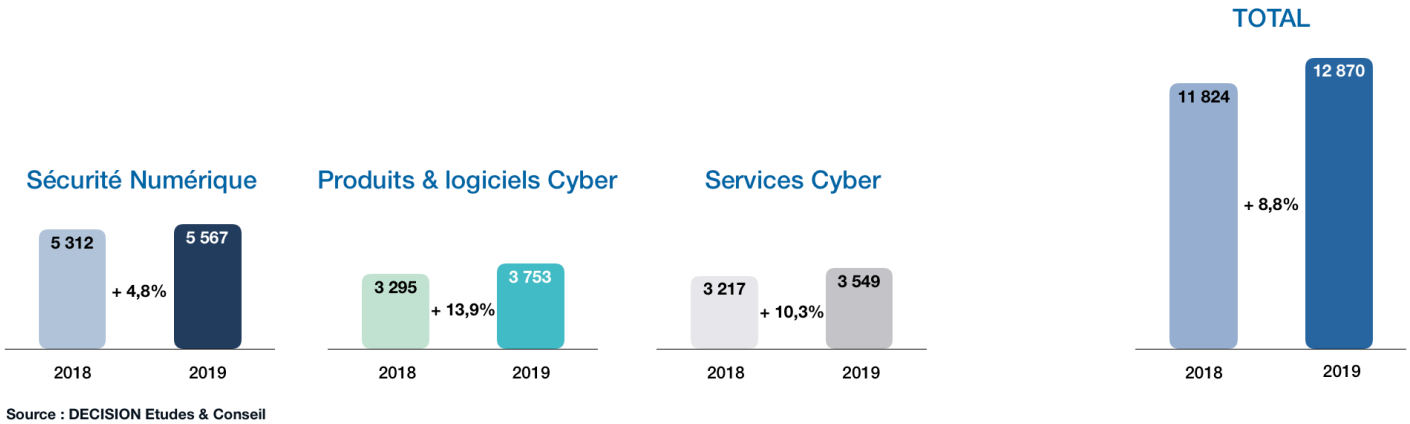
III) Les chiffres clés de la filière

3.1 Analyse par sous-segment

3.1.a. Taille et croissance 2014-2019

CA de la Confiance Numérique par Segment 2018-2019 (Millions d'euros)





Source : DECISION Etudes & Conseil

CA de confiance numérique en france : 12,9 Mds € en 2019

III) Les chiffres clés de la filière

3.1.b. Valeur Ajoutée en 2019

VALEUR AJOUTÉE EN FRANCE EN 2019 PAR SEGMENT

SÉCURITÉ NUMÉRIQUE

2 282 M€

+

PRODUITS DE CYBERSÉCURITÉ

2 182 M€

+

SERVICES DE CYBERSÉCURITÉ

1 644 M€

=

N°	SEGMENT	VALEUR AJOUTÉE EN 2019 EN MILLIONS D'EUROS
1.2.1.1	CONTROLE D'ACCES	553
1.2.1.2	IDENTIFICATION DES PERSONNES	795
1.2.6	OBSERVATION LARGE ZONE	287
1.2.7	SUIVI - TRAÇAGE - LOCALISATION	183
1.2.9	COMMANDE - CONTRÔLE - AIDE À LA DÉCISION	286
1.2.10	RENSEIGNEMENT - COLLECTE D'INFORMATION	178
2.0.1	GOUVERNANCE	350
2.0.2	GESTION DES IDENTITÉS ET DES ACCÈS	394
2.0.3	SÉCURITÉ DES DONNÉES	593
2.0.4	SÉCURITÉ DES APPLICATIONS	172
2.0.5	SÉCURITÉ DES INFRASTRUCTURES	542
2.0.6	SÉCURITÉ DES PRODUITS & ÉQUIPEMENTS	131
3.0.1	AUDIT - PLANNING - CONSEIL	638
3.0.2	MISE EN OEUVRE CYBERSÉCURITÉ	486
3.0.3	INFOGÉRANCE - EXPLOITATION	453
3.0.4	FORMATION EN CYBERSÉCURITÉ	67

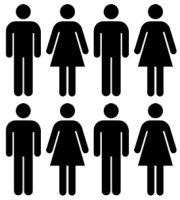
Source : DECISION Etudes & Conseil

6 110 M€ DE VA DE CONFIANCE NUMÉRIQUE EN FRANCE

III) Les chiffres clés de la filière

3.1.c. Emplois en 2019

EMPLOIS EN FRANCE EN 2019 PAR SEGMENT



SÉCURITÉ NUMÉRIQUE

25 300

+

PRODUITS DE CYBERSÉCURITÉ

18 790

+

SERVICES DE CYBERSÉCURITÉ

21 650

=

N°	SEGMENT	EMPLOIS EN 2019
1.2.1.1	CONTROLE D'ACCES	6 440
1.2.1.2	IDENTIFICATION DES PERSONNES	8 500
1.2.6	OBSERVATION LARGE ZONE	2 490
1.2.7	SUIVI - TRAÇAGE - LOCALISATION	2 420
1.2.9	COMMANDE - CONTRÔLE - AIDE À LA DÉCISION	3 260
1.2.10	RENSEIGNEMENT - COLLECTE D'INFORMATION	2 190
2.0.1	GOUVERNANCE	3 760
2.0.2	GESTION DES IDENTITÉS ET DES ACCÈS	2 790
2.0.3	SÉCURITÉ DES DONNÉES	5 200
2.0.4	SÉCURITÉ DES APPLICATIONS	1 120
2.0.5	SÉCURITÉ DES INFRASTRUCTURES	4 610
2.0.6	SÉCURITÉ DES PRODUITS & ÉQUIPEMENTS	1 310
3.0.1	AUDIT - PLANNING - CONSEIL	9 710
3.0.2	MISE EN OEUVRE CYBERSÉCURITÉ	7 200
3.0.3	INFOGÉRANCE - EXPLOITATION	3 810
3.0.4	FORMATION EN CYBERSÉCURITÉ	930

Source : DECISION Etudes & Conseil

65 740 EMPLOIS DE CONFIANCE NUMÉRIQUE EN FRANCE

III) Les chiffres clés de la filière

3.1.d. Nombre d'entreprises en 2018

NOMBRE D'ENTREPRISES EN FRANCE EN 2019 PAR SEGMENT

SÉCURITÉ NUMÉRIQUE
1 700

PRODUITS DE CYBERSÉCURITÉ
692

SERVICES DE CYBERSÉCURITÉ
681

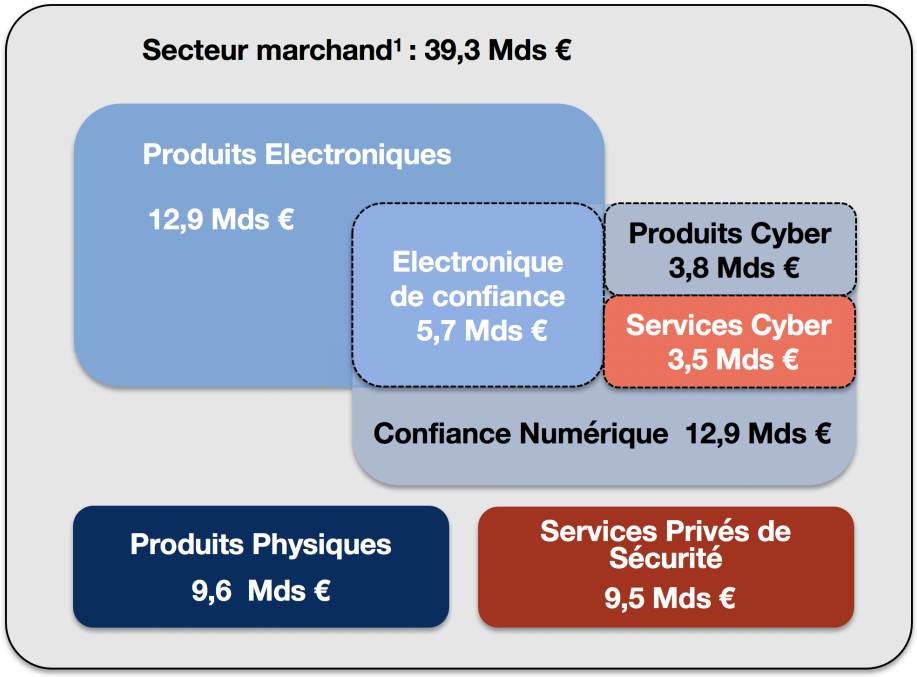
N°	SEGMENT	NOMBRE D'ENTREPRISES EN 2019
1.2.1.1	CONTROLE D'ACCES	324
1.2.1.2	IDENTIFICATION DES PERSONNES	486
1.2.6	OBSERVATION LARGE ZONE	191
1.2.7	SUIVI - TRAÇAGE - LOCALISATION	222
1.2.9	COMMANDE - CONTRÔLE - AIDE À LA DÉCISION	267
1.2.10	RENSEIGNEMENT - COLLECTE D'INFORMATION	214
2.0.1	GOUVERNANCE	204
2.0.2	GESTION DES IDENTITÉS ET DES ACCÈS	203
2.0.3	SÉCURITÉ DES DONNÉES	325
2.0.4	SÉCURITÉ DES APPLICATIONS	157
2.0.5	SÉCURITÉ DES INFRASTRUCTURES	325
2.0.6	SÉCURITÉ DES PRODUITS & ÉQUIPEMENTS	156
3.0.1	AUDIT - PLANNING - CONSEIL	637
3.0.2	MISE EN OEUVRE CYBERSÉCURITÉ	435
3.0.3	INFOGÉRANCE - EXPLOITATION	340
3.0.4	FORMATION EN CYBERSÉCURITÉ	209

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

2 134 ENTREPRISES DE CONFIANCE NUMÉRIQUE EN FRANCE

3.2 Comparaison avec les autres secteurs de la sécurité en France

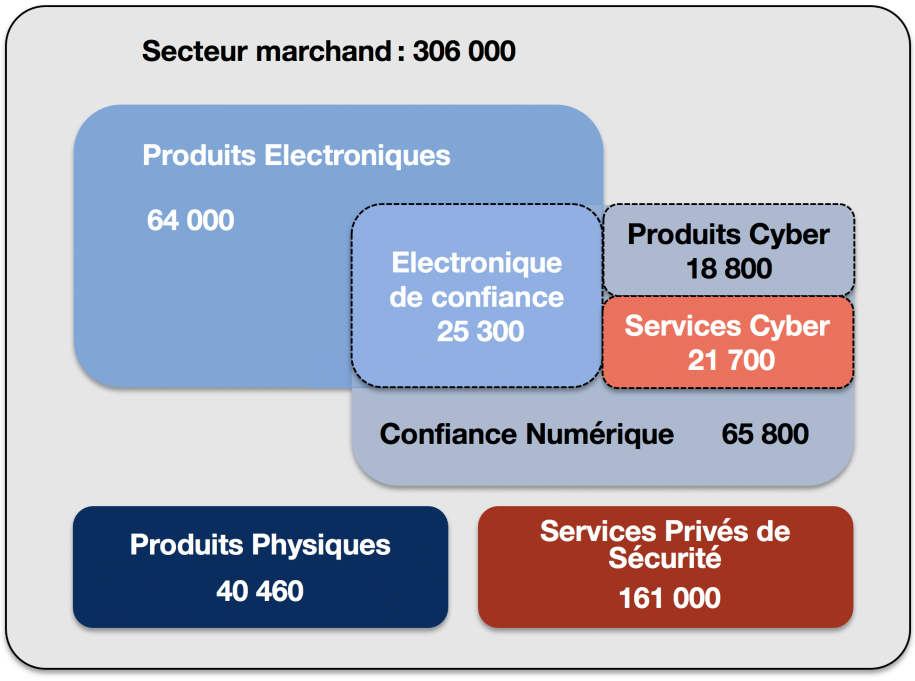
CA France de la filière de sécurité en 2019



[1] La filière marchande réalise aussi plus de 9 Mds € de CA à travers les filiales des entreprises de capitaux français à l'étranger

Source : DECISION Etudes & Conseil

Emplois en France de la filière de sécurité en 2019



Source : DECISION Etudes & Conseil

IV) Les tendances de marché

4.1 Tendances de marché sur la période 2017-2020

4.1.a. De nombreux mouvements de fusion-acquisition

Au sein de la filière de la Confiance Numérique, 68 rachats d'entreprises concernant des sièges d'entreprises localisés en France ont été recensés sur la période 2017-2020 (soit en moyenne 22 rachats par an). Ces achats concernent aussi bien des achats inter-entreprises que des achats d'entreprises par des fonds financiers et des achats entre fonds financiers.

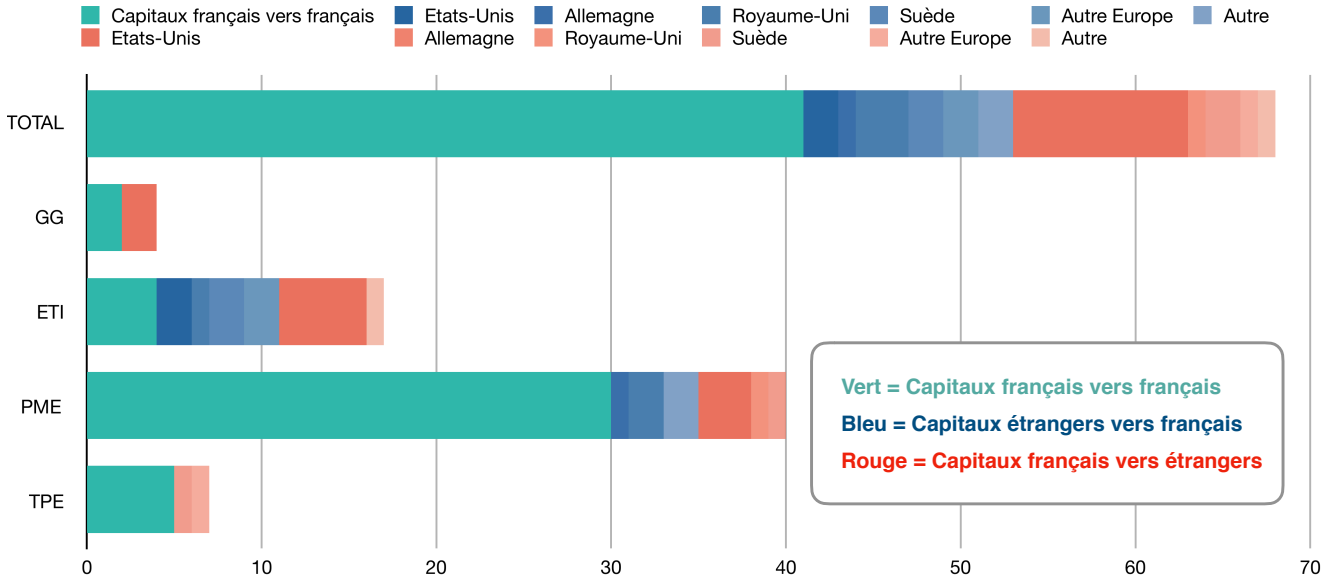
Parmi eux:

- 41 rachats d'entreprises françaises par d'autres entreprises françaises (60%)
- 12 rachats d'entreprises étrangères par des entreprises françaises (18%)
- 15 rachats d'entreprises françaises par des entreprises étrangères (22%)

La grande majorité des entreprises rachetées sont des PME (59%) et des ETI (25%), en croissance.

Le nombre de rachats d'entreprises françaises par des capitaux étrangers est supérieur de 25% sur la période au nombre de rachats d'entreprises étrangères par des entreprises de capitaux français. La taille moyenne des entreprises rachetées est également au profit des capitaux étrangers.

Enfin, les deux-tiers des rachats d'entreprises françaises par des entreprises étrangères s'opère au profit de capitaux américains (67%). De plus, les rachats aux profits de capitaux américains concernent de loin les rachats les plus importants sur la période en comparaison des autres pays en termes de taille d'entreprises rachetées : Oberthur Technologies (Advent) puis Safran Morpho (Advent) fusionné avec Oberthur Technologies, Hensoldt, Arismore, Nexeya, Fichet Group, nCipherSecurity, etc. Les 68 mouvements de rachats sont résumés dans le diagramme ci-dessous :



- **GG** = Grande entreprise (Groupe) : Dans le monde, CA > 1,5 milliard d'euros *ou* nombre d'employés > 1500
- **ETI** = Entreprise de Taille Intermédiaire : Dans le monde, CA > 50 millions d'euros *ou* nombre d'employés > 250
- **PME** = Petite ou Moyenne Entreprise: Dans le monde, CA > 2 millions d'euros *ou* nombre d'employés > 10
- **TPE** = Très Petite Entreprise: Dans le monde, CA < 2 millions d'euros *et* nombre d'employés < 10

IV) Les tendances de marché

Les principaux mouvements de fusions-acquisitions sur la période 2017-2020 sont présentés ci-dessous.

Principaux rachats entre entreprises de capitaux français sur la période 2017-2020

Année	Entreprise acheteuse		Entreprise achetée		
	Nom	Taille de l'entreprise	Nom	Taille de l'entreprise	Activité
2020	**Sopra Steria**	GG	Sodifrance	ETI	Conseil en transformation numérique. Une partie de l'activité est dédiée au conseil en cybersécurité : Audit, test, conseil, évaluation de la conformité aux standards, formation, service SOC
2019	**Thales**	GG	Gemalto	GG	Solutions d'identification & authentification : paiements sécurisés, sécurisation des IoTs, biométrie, etc.
2019	**Cap Gemini**	GG	Altran	GG	Services d'ingénierie et de R&D, y compris pour la filière de sécurité
2019	**IN Groupe**	ETI	Surys	ETI	Solutions d'identification & authentification
2019	**Atos**	GG	Idnomic	PME	Infrastructures de gestion des identités numériques
2018	**Butler Industries**	Fond	NextiraOne (NXO)	ETI	Conseil en transformation numérique. Une partie de l'activité est dédiée au conseil en cybersécurité
2018	**Suneris** (Filiale de Thales)	GG	ERCOM	PME	Producteur de solutions de chiffrement des communications
2018	**Groupe CS**	ETI	Novidy's	PME	Services de cybersécurité : Conseil, intégration de solutions de sécurité et services managés
2017	**Sopra Steria**	GG	Galitt	ETI	Logiciels de paiement / transactions sécurisées
2014-2019	**Vivaprotect**	ETI	Vauban Systems, TDSI, ARD	PMEs	Née en 2014 de la fusion entre TIL Technologies et Sorphea, l'entreprise française Vivaprotect soutenue par le fond Eurazeo et la BPI multiplie les achats en 2019 avec les deux PME françaises Vauban Systems et ARD ainsi que la PME anglaise TDSI (trois acteurs de la confiance numérique).

Principales fusions et Joint Ventures concernant des entreprises françaises

Parmi les principaux mouvements de fusion sur la période 2017-2020 :

- En 2018, ULIS et Sofradir, leaders français des capteurs infrarouges, fusionnent pour former Lynred. Les deux entreprises ainsi réunies étaient et demeurent la propriété de Thales et de Safran.
- En 2019, Naval Group et Fincantieri ont signé l'accord de co-entreprise qui, en janvier 2020, a entrainé la création de Naviris, une co-entreprise détenue à parts égales par les deux groupes et qui a vocation de diriger des projets binationaux et des projets d'exportation. Les navires conçus par Naval Group intègrent une proportion croissante de solutions de cybersécurité.

IV) Les tendances de marché

Principaux rachats d'entreprises de capitaux étrangers par des entreprises de capitaux français sur la période 2017-2020

Année	Entreprise acheteuse			Entreprise achetée			
	Nom	Taille de l'entreprise	Nationalité	Nom	Taille de l'entreprise	Nationalité	Activité
2020	**IN Groupe**	ETI	France	Nexus	ETI	Suède	Identification des personnes et des objets. Plateforme PKI, Card Management System, etc.
2019	**Orange Cyberdefense**	GG	France	Securelink	ETI	Pays-Bas	Conseil en cybersécurité
2019	**Orange Cyberdefense**	GG	France	SecureData	ETI	Royaume-Uni	Conseil en cybersécurité
2019	**Cap Gemini**	GG	France	Leidos cyber	ETI	Etats-Unis	Conseil en cybersécurité : offres intégrées, services de sécurité managés…
2019	**Inside Secure** *(spin-off de Gemalto)*	ETI	France	Verimatrix	ETI	Etats-Unis	Solutions de sécurité pour appareils mobiles et connectés
2018	**Latour Capital** (*accompagné par BPI France)*	Fond	France	Sogetrel *(Fond Quilvest)*	ETI	Luxembourg	Déploiement de réseaux Très Haut Débit, la sureté électronique, les objets connectés…
2018	**Idemia**	GG	France	Otono Networks	PME	Canada	Spécialiste des solutions de gestion et d'orchestration des SIM embarquées (eSIM)
2018	**Sopra Steria**	GG	France	Bluecarat	PME	Allemagne	Conseil stratégique dans le domaine technologique, de la cybersécurité et de l'API Management.
2017	**Sopra Steria**	GG	France	Kentor	ETI	Suède	Conseil en cybersécurité

IV) Les tendances de marché

Principaux rachats d'entreprises de capitaux français par des entreprises de capitaux étrangers sur la période 2017-2020

Année	Entreprise acheteuse			Entreprise achetée			
	Nom	Taille de l'entreprise	Nationalité	Nom	Taille de l'entreprise	Nationalité	Activité
2019	**Hensoldt** *(Fond américain KKR)*	GG	Etats-Unis	Nexeya	ETI	France	Systèmes de navigation, guidage et optronique, simulation, surveillance, détection er renseignement
2019	**Cisco**	GG	Etats-Unis	Sentryo	PME	France	Fournisseur de logiciels de solutions de cybersécurité pour réseaux d'IoTs industriels
2019	**GFI Informatique**	GG	Qatar	SIS	PME	France	La Société d'Informatique et de Systèmes (SIS), est concepteur de logiciels de gestion de l'urgence (régulation des appels d'urgence utilisée par les SAMU, système d'alerte, gestion opérationnelle et d'aide à la décision des pompiers)
2018	**Marque Idemia** *(Fond Advent International)*	GG	Etats-Unis	Morpho (Safran)	ETI	France	Identification et authentification, biométrie, sécurité digitale, analyse de données et de vidéos
2018	**Tsinghua Unigroup**	GG	Chine	Linxens	ETI	France	En amont de la filière : Spécialiste français des connecteurs et antennes radio de cartes à puce
2017	**Hensoldt** *(Fond américain KKR)*	GG	Etats-Unis	Activité « Defence Electronics » d'Airbus D&S	GG	France	Capteurs critiques (radars, optronique, etc.), systèmes de guerre électronique et d'avionique (y compris drones) pour applications de Défense et de Sécurité
2017	**Accenture**	GG	Etats-Unis	Arismore	ETI	France	Services de cybersécurité*

*Ce rachat s'inscrit dans une politique ambitieuse de croissance externe sur le secteur de la cybersécurité entamée par Accenture au niveau mondial depuis 2015 avec les rachats successifs de Fusionx, Cimation, Maglan, Redcore, Defense Point, Endgame Federal Services, iDefense, Deja Vu Security ainsi que l'ancienne division Cyber Security Service de Symantec rachetée à Broadcom en 2020. L'ensemble de ces opérations représente près de 1500 employés venant grossir les rangs d'Accenture sur le segment de la cybersécurité dans le monde.

Autres mouvements intéressants pour la filière française

Précisons le rachat en 2019 de la branche « Security business » de Symantec par Broadcom pour 10,7 milliards de dollars. Symantec conserve son portefeuille de produits destinés au grand-public, qui comprend la marque de protection d'identité LifeLock et le logiciel antivirus Norton. En conséquence, Symantec reste présent en France en tant qu'entreprise de taille intermédiaire mais se renomme NortonLifeLock.

Le Groupe Fichet -historiquement français et racheté par le Suédois Gunnebo au tournant des années 2000- a été racheté par le fonds d'investissement américain OpenGate Capital en décembre 2018. L'entreprise est historiquement spécialisée dans la serrurerie et les coffre-forts bancaires. Pour faire face à la faible croissance de ce marché, l'entreprise tente de diversifier ses marchés (protection des sites sensibles, cash management pour retail, etc.), ainsi que son offre (vers un contrôle d'accès au sens large, y compris électronique), la sécurisation des sites sensibles. Depuis le rachat, l'entreprise est renommée sous le nom de Fichet Security Solutions et représentait un chiffre d'affaires de 137 M€ en 2018 pour 850 salariés.

Enfin, les grands acteurs de la sécurité privée se positionnent de plus en plus sur des segments de la Confiance Numérique, qui bénéficient de meilleurs taux de marges et s'intègrent avantageusement dans leurs offres de sécurité privée -vers des offres globales de sécurité externalisées. A titre d'exemple, la grande entreprise espagnole Prosegur, l'un des leaders européens du gardiennage, 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.

4.1.b. Les quelques entreprises en faillite

La Confiance Numérique est portée par une très forte croissance et ne souffre donc que d'un très faible nombre de faillites, concentré exclusivement sur des PME et TPE. Le tableau ci-dessous montre les deux PME concernées sur la période 2018-2019.

Année	Taille de l'entreprise	Entreprise	Activité
2019	PME	**SILKAN RT**	Conception de composants, systèmes électroniques et logiciels embarqués de simulation, de communication en temps réel et de transmission rapide de données (par exemple pour les drones). Poursuite de l'activité d'Agueris, co-entreprise crée avec le Groupe CMI
2018	PME	**SAFETIC** *(ETUDE ET DEVELOPPEMENTS EN ELECTRONIQUE)*	Solutions de contrôle d'accès, y compris biométrique. Clôture définitive suite à des difficultés depuis 2012

4.2 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 deux manières différentes et complémentaires.

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

Les innovations issues des industries électronique et numérique impactent presque tous les secteurs des économie modernes et génèrent de ce fait des 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 là « *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 (Etats-Unis) dans les processeurs et SK Hynix (Corée du Sud), Micron (Etats-Unis) et Toshiba (Japon) dans les mémoires. En conséquence de la miniaturisation et de la baisse des coûts, les produits électroniques se démocratisent, y compris en matière de confiance numérique : capteurs, système de traçage et localisation, ainsi que tous les sous-systèmes inclus dans les segments électroniques de la filière.

- **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 Etats-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 croient 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 pour la France et 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 cards, 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 associées de bout-en-bout. 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 par des acteurs de capitaux majoritairement européens 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.

4.2.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 à crypter 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, distribution quantique de clefs), 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, 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 cartes à puce sans contact, 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 entrain d'être développées et mises en place.

   - **Cryptographie quantique et 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, deux axes principaux et complémentaires se développent : d'une part, la cryptographie post-quantique, qui se base sur de nouveaux concepts mathématiques pour chiffrer les protocoles de communication, d'autre part, la cryptographie quantique, qui utilise les propriétés de la physique quantique pour sécuriser le transport de l'information. La cryptographie quantique est à court terme le champ d'application le plus prometteur des développements quantiques. Les premières applications industrielles sont en train d'être développées et mises en place.

   - **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 cryptage entièrement homomorphe (FHE) permet le calcul sur des données cryptées 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 crypté, 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 voir quelques années.

- **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 / ou de matériel (HW) et visant à être intégrés dans des dispositifs communicants afin de gérer de manière sécurisée toutes les interactions entre ces derniers et le monde extérieur en stockant des applications dédiées et des données confidentielles de manière chiffrée (cartes SIM, puces de cartes bancaires…). Dans le contexte du développement des IoT, le segment des éléments sécurisés est marqué par le remplacement des cartes SIM (Universal integrated circuit card), par des éléments sécurisés miniaturisés et directement embarqués ou intégrés dans les systèmes auxquels ils se rattachent, voir 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**.

IV) Les tendances de marché

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.

5. **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.

6. **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.

7. **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.

8. 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**…

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

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

En effet, au niveau mondial, 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 ;

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 des services privés est donc de diversifier leurs services en y intégrant des produits électroniques et cyber et en montant en gamme. A titre illustratif, la grande entreprise espagnole Prosegur, l'un des leaders européens du gardiennage -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.

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

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

Thales, à travers le rachat de Gemalto 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.

4.3.3 …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.

4.3.4 … 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 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 ses 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.

IV) Les tendances de marché

4.4 Le potentiel de croissance offert par l'identité numérique

4.4.a. L'identité numérique

L'identité numérique a pour définition, au sein de l'ACN, les 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, 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.

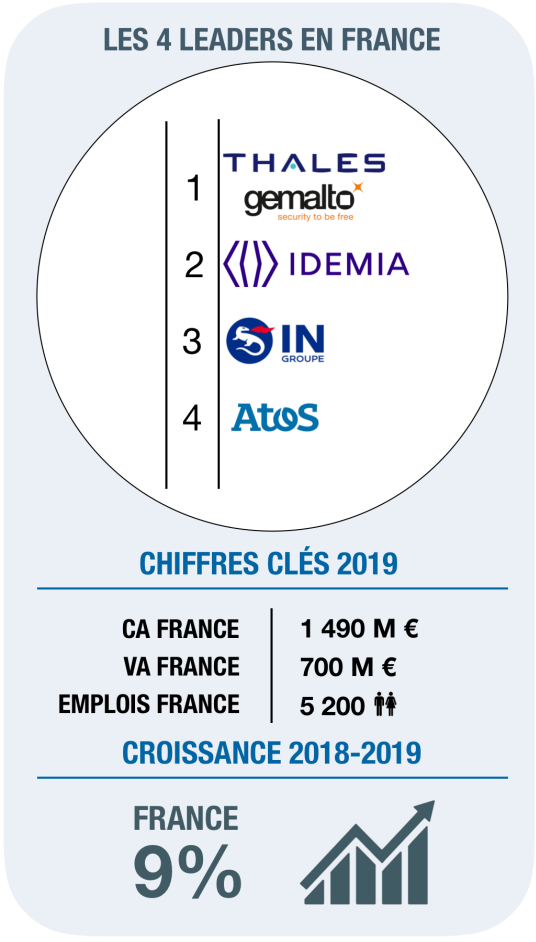
4.4.b. Un marché mondial porteur

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 pour 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, recourant 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.

4.4.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 : 1,5 milliards d'euros en 2019, pour 5 200 emplois et une valeur ajoutée de 700 millions d'euros.

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

IV) Les tendances de marché

4.4.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), devant commencer à être déployée en août 2021, le support d'une identité numérique de niveau élevé ;
- 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.

IV) Les tendances de marché

4.5 Cybersécurité : un paysage législatif européen qui s'étoffe

La cybersécurité, et plus largement le numérique, fait depuis plusieurs années l'objet d'un foisonnement législatif intense visant à inciter l'ensemble des usagers du numérique à prendre conscience du caractère stratégique de la protection des données, personnelles ou non, issues de leurs activités.

Ainsi, à l'image de la France, pays précurseur dans ce domaine, l'Union européenne s'est dotée ces dernières années de plusieurs outils législatifs pour accompagner l'ensemble des acteurs économiques dans leur nécessaire cyber-sécurisation, notamment à travers la directive NIS (Network and Information Security) qui fait peser un certain nombre d'obligations sur les OSE (Opérateurs de Services Essentiels).

Cette brique de départ a depuis été complétée par le règlement RGPD (Règlement Général sur les Données Personnelles) ainsi que par le règlement « European Cybersecurity Act », définitivement adopté en Mai 2019 et qui vient poser de nouvelles règles encadrant la certification en matière de cybersécurité au niveau européen (voir la note d'analyse détaillée et Position ACN publiée sur le sujet).

Le European Cybersecurity Act définit un cadre clair et harmonisé pour la mise en œuvre de la cybersécurité dans tous les secteurs économiques. En effet, l'édiction de règles communes en matière de certification en cybersécurité au niveau européen constitue une avancée primordiale pour permettre le développement d'un marché européen unifié au bénéfice des PME et des grands groupes de la confiance numérique.

L'ensemble de ces textes, incluant également le niveau national avec la mise en œuvre effective des décrets d'application de la LPM (Loi de Programmation Militaire) décrivant les obligations, en matière de cybersécurité, des OIV (Organismes d'Importance Vitale), sont de nature à accélérer la prise de conscience générale autour de la nécessité d'intégrer la cybersécurité à toutes les activités.

Cette prise de conscience sera probablement un support considérable au développement du marché et des entreprises de la confiance numérique qui peuvent compter sur une demande soutenue et ce pour une période durable.

La faculté du secteur d'établir des référentiels de cybersécurité adaptés susceptibles d'être portés au niveau européen (certification puis standardisation/normalisation en lien avec chaque secteur utilisateur et avec l'appui de l'ANSSI), est cruciale pour générer de nouveaux relais de croissance à long terme.

4.6 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 (grands concerts), diplomatiques (G7, G20, etc.), est un thème particulier qui nécessite un ensemble de capacités (contrôle d'accès, gestion des flux, coordination des forces, cybersécurité, 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 mène actuellement 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 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. 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…

IV) Les tendances de marché

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'étendrons 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.

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.

4.7 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 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)*
- *Segment 2.0.5 : Sécurité des infrastructures*
  - La mise à jour du firmware
  - L'authentification, c'est-à-dire la séquence d'authentification machine-to-machine

Les acteurs de la filière interrogés 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.

IV) Les tendances de marché

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 en 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.

4.8 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. **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 9% par an sur la période 2014-2019.
- 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 2016-2020.

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 12,4 Milliards d'euros de chiffre d'affaires dans ce secteur en forte croissance (9% de croissance chaque année depuis 2014).

Les membres de l'Alliance pour la Confiance Numérique (ACN), dont 65% de PME/TPE-ETI, représentent plus de 70% du chiffre d'affaires du secteur de la Confiance Numérique repartis sur l'ensemble de la chaine de valeur (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, en cours de création.

Par ailleurs, l'ACN est également membre fondateur du partenariat Public Privé de la Cybersécurité porté par l'association l'ECSO (*European CyberSecurity Organisation*).

Liste des membres

Advanced Track&Trace, AIRBUS, AMOSSYS, ARIADNEXT, Atos, business card associates, BYSTAMP, Capgemini, CERTIGNA Services de confiance numérique, Certinomis, ChamberSign, CLR Labs, CS, cryptr, egidium TECHNOLOGIES, DOCAPOSTE, ELYCTIS e-ID expert, BlueFiles, GUARDEA, ICUBE, IDEMIA, IN GROUPE, KAT, LEX persona Trust each other, NOKIA, obdo own your data, Oveliane, RED ALERT LABS IoT Security, rubycat, SERMA SAFETY & SECURITY, SIFARIS, sopra steria, life.augmented, SYSDREAM Division Cybersécurité Hub One, TEHTRIS, THALES, TIXEO, YESWEHACK, zama, ziwit

Partenaires

cea, EUROSMART The Voice of the Smart Security Industry, Inria inventeurs du monde numérique, BRETAGNE DÉVELOPPEMENT INNOVATION, POLE SCS

A propos de DECISION Etudes & Conseil

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.

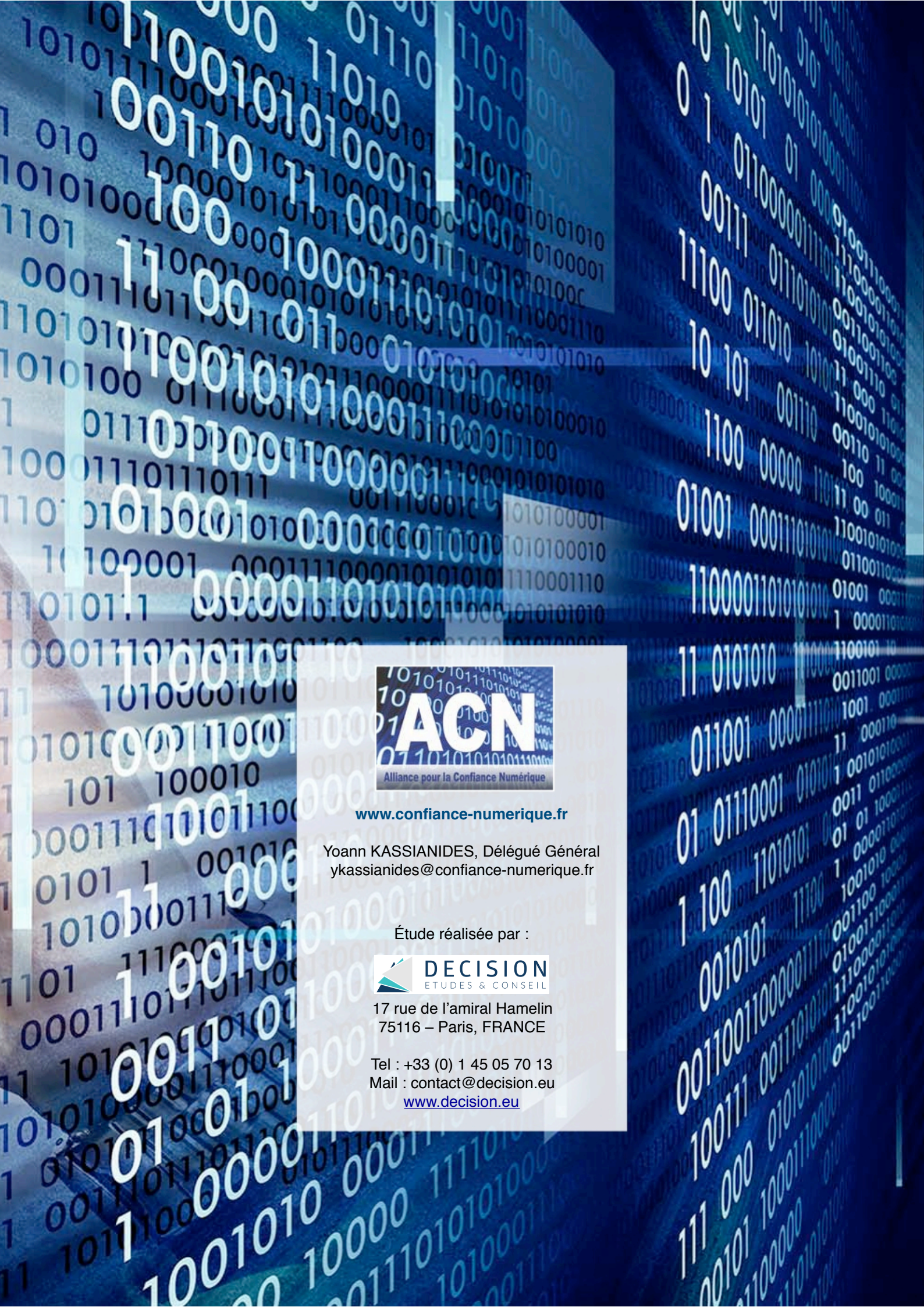
Nos clients regroupent des entreprises privées, que cela soit des startups/PME/ETI, des grands groupes industriels, des organisations professionnelles ou des institutions financières et des fonds d'investissements, mais également les pouvoirs publics locaux et nationaux (gouvernements, ministères, etc.)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

En 2009, DECISION initie et conduit la première étude pour la Commission européenne sur l'industrie de sécurité. Partenaire 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 l'étude d'évaluation du poids économique de la filière de sécurité pour le gouvernement français en 2015 (sous l'égide du PIPAME, structure inter-ministérielle regroupant le Ministère de l'Economie, le Ministère de l'Intérieur et le SGDSN) qui a été ré-actualisée en 2018. En 2017, 2019 et 2020, DECISION conduit également l'Observatoire pour l'Alliance pour la Confiance Numérique (ACN).

Pour plus d'informations :

www.decision.eu

DECISION
ETUDES & CONSEIL



www.confiance-numerique.fr

Yoann KASSIANIDES, Délégué Général
ykassianides@confiance-numerique.fr

Étude réalisée par :

DECISION ETUDES & CONSEIL
17 rue de l'amiral Hamelin
75116 – Paris, FRANCE

Tel : +33 (0) 1 45 05 70 13
Mail : contact@decision.eu
www.decision.eu