L'Observatoire de la filière de la Confiance Numérique

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

2019

Sommaire

Etude définie et commanditée par l'**Alliance pour la Confiance Numérique (ACN)**
dans le cadre de son Observatoire 2019

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**

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 2019, couvrant le champ de la cybersécurité et de la sécurité numérique.

La Confiance Numérique en France en 2018 c'est :

- **12,4 milliards d'euros de chiffre d'affaires** réalisé en France, soit 9,1% de croissance 2018-2017
- **5,8 milliards d'euros de valeur ajoutée** réalisée en France, soit 7,4% de croissance 2018-2017
- **52 300 personnes employées** dans le secteur, soit 4,4% de croissance 2018-2017
- Un **chiffre d'affaires** réparti à **55% pour la Cybersécurité et à 45% pour la Sécurité Numérique**

Les entreprises françaises de la Confiance Numérique dans le Monde en 2018 c'est :

- **16,9 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 sécurisation des paiements et de la gestion des identités et des accès *(biométrie, cartes à puce, terminaux de paiement, etc.).*
- **9,1 milliards d'euros de chiffre d'affaires à l'international**, soit 54% du CA total *(CA exporté depuis la France et CA réalisé à l'étranger par des entreprises détenues par des capitaux français)*
- **4,6 milliards d'euros de chiffre d'affaires à l'exportation depuis la France**, soit un taux d'export moyen de 37%

La Confiance Numérique est une filière à part entière :

- **9%** de croissance moyenne annuelle en France sur la période 2013-2018, contre **1,4%** 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 :

- **2 088 entreprises** dans la filière en France
- Dont **65 grandes entreprises**
- Dont **75 ETI** (Entreprises de Taille Intermédiaire)
- Dont **636 PME** (Petites et Moyennes Entreprises)
- Dont **1 312 micro-entreprises**, générant moins de 2 millions de CA en 2018

Éléments clefs

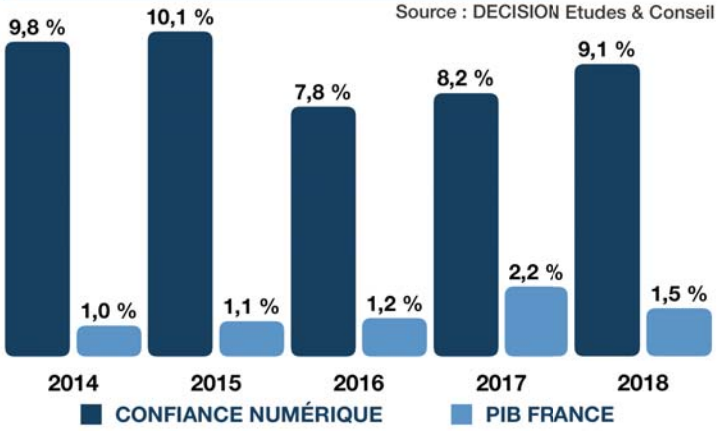
FONDAMENTAUX 2018

CA MONDE	16,9 MDS €	CROISSANCE 2017-2018
CA HORS DE FRANCE	4,5 MDS €	9,1%
CA FRANCE	12,4 MDS €	
DONT CA EXPORT	4,6 MDS €	52 300 EMPLOIS EN FRANCE
VA FRANCE	5,8 MDS €	
MARCHÉ FRANÇAIS	10,3 MDS €	

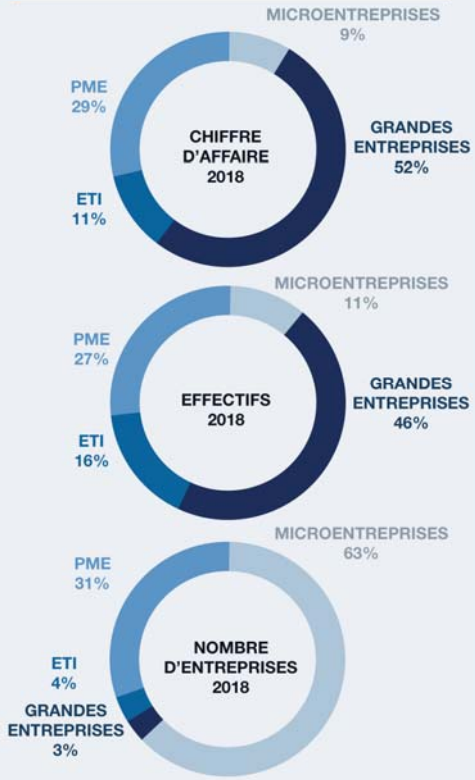
Source : DECISION Etudes & Conseil

CROISSANCES COMPARÉES 2013-2018

Source : DECISION Etudes & Conseil

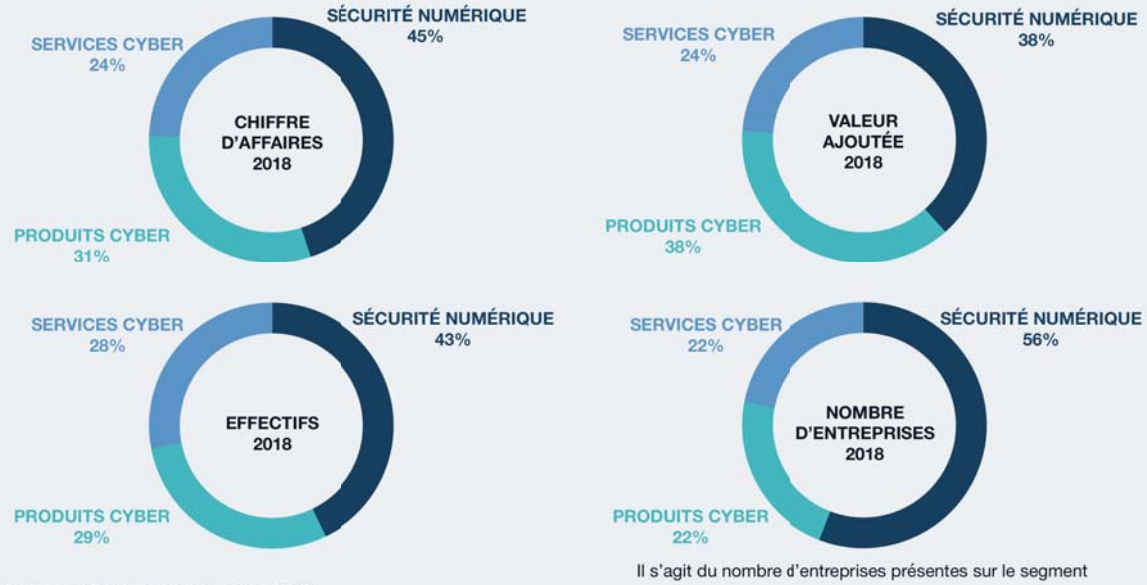


ANALYSE PAR TAILLE D'ENTREPRISES



Source : DECISION Etudes & Conseil

LES PRINCIPAUX SEGMENTS DE LA CONFIANCE NUMÉRIQUE



Source : DECISION Etudes & Conseil

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

Éléments clefs

TOP 10 ACTEURS FRANCE

N°	ENTREPRISE	CA CONFIANCE NUMÉRIQUE FRANCE	CA CONFIANCE NUMÉRIQUE MONDE	N° MONDE
1	THALES & GEMALTO	1 610 M €	4 260 M €	1
1	THALES	827 M €	1 392 M €	1
1	GEMALTO	784 M €	2 868 M €	1
2	IDEMIA	668 M €	2 640 M €	2
3	AIRBUS D&S	479 M €	570 M €	6
4	ATOS	381 M €	785 M €	4
5	IBM	259 M €	2 155 M €	3
6	ORANGE CYBERDEFENSE	191 M €	521 M €	7
7	IN GROUPE	177 M €	283 M €	9
8	CAP GEMINI	172 M €	687 M €	5
9	SOPRA STERIA	138 M €	315 M €	8
10	ENGIE	133 M €	133 M €	10

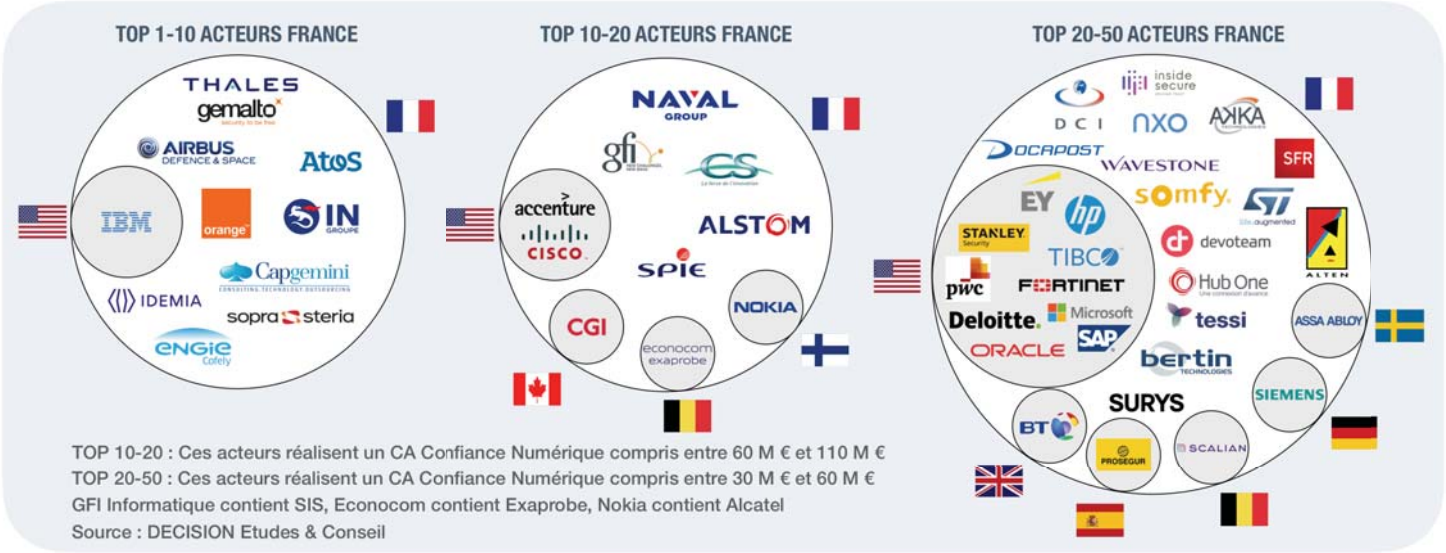
Source : DECISION Etudes & Conseil

Cap Gemini inclut les chiffres de Sogeti - Orange cyberdéfense inclut les chiffres de Securelink

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;
- **Gemalto** 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, Mai 2019), 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 en France ;
- Enfin, les activités de confiance numérique d'**ENGIE** sont dispersées mais couvrent l'ensemble de la filière, de la sécurité numérique à la cybersécurité.

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.



TOP 10-20 : Ces acteurs réalisent un CA Confiance Numérique compris entre 60 M € et 110 M €
TOP 20-50 : Ces acteurs réalisent un CA Confiance Numérique compris entre 30 M € et 60 M €
GFI Informatique contient SIS, Econocom contient Exaprobe, Nokia contient Alcatel
Source : DECISION Etudes & Conseil

I) Confiance Numérique :
Cybersécurité et Sécurité Numérique

1.1 Cybersécurité et Sécurité Numérique : deux domaines complémentaires

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

L'Observatoire de la Confiance Numérique couvre deux industries :

- La **Cybersécurité** proprement dite, qui correspond à la sécurisation «interne» des systèmes numériques. La cybersécurité regroupe deux types d'activités souvent associées dans la pratique, les services (conseil, conception, mise en place, exploitation, formation), et les logiciels et solutions, destinés aux marchés professionnels (Etat et secteur public, installations critiques, entreprises, PME) et grand public (ordinateurs, smartphones, maison, véhicules et objets connectés, etc).
- La **Sécurité Numérique**, c'est-à-dire les produits et solutions électroniques de mise en œuvre de systèmes numériques pour instaurer la confiance dans le monde extérieur. Ces systèmes mettent en œuvre des moyens numériques sécurisés pour instaurer la confiance dans l'environnement citoyen, en particulier par la gestion des identités, la gestion des accès, la biométrie, les transactions, les 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.

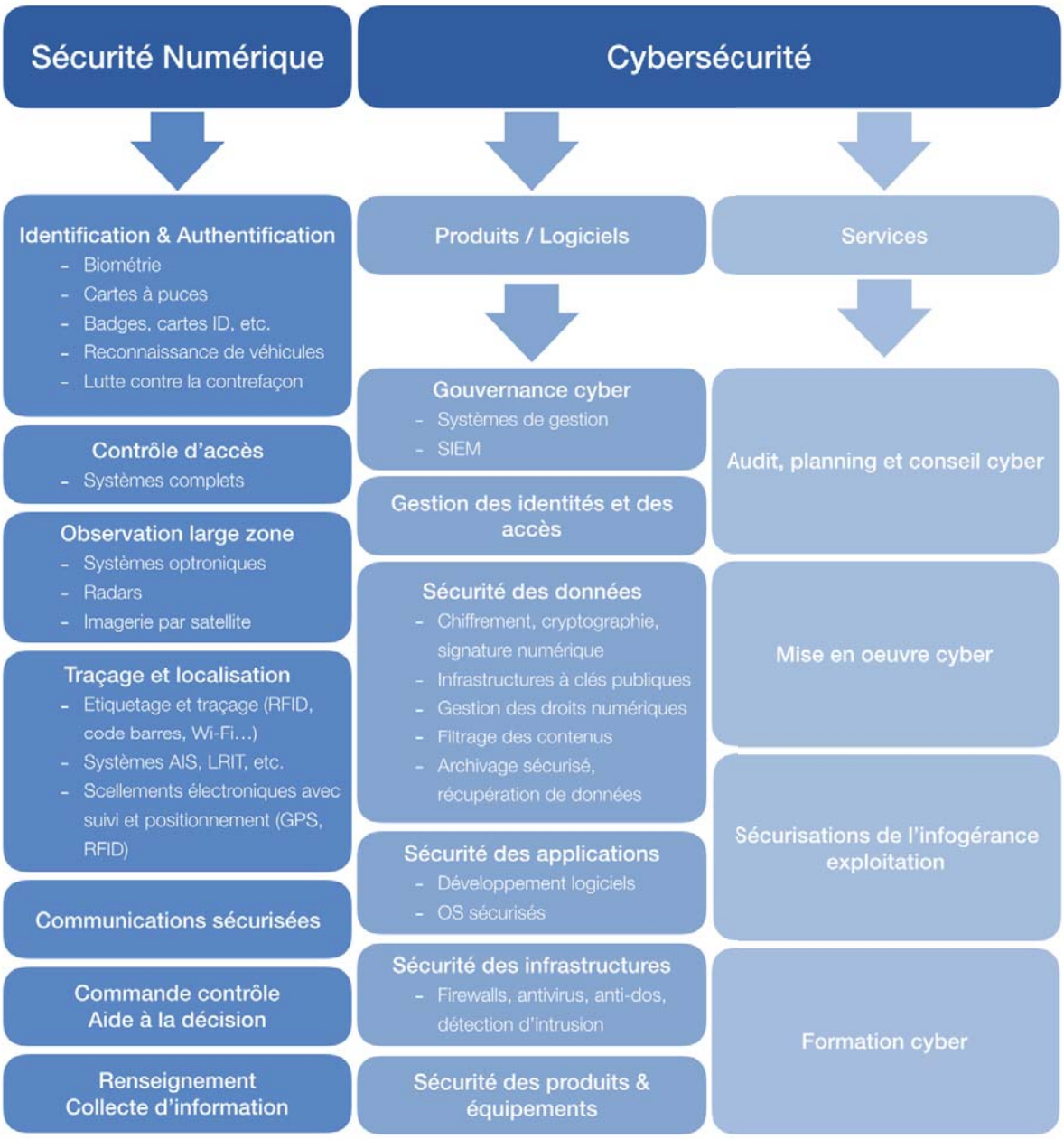
I) Confiance Numérique :
Cybersécurité et Sécurité Numérique

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

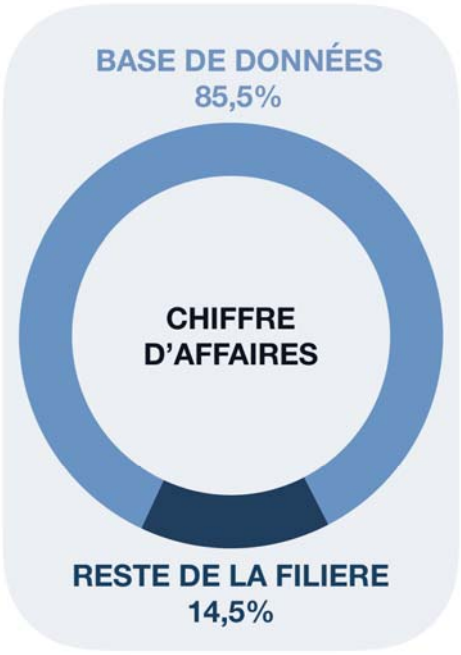
1.3 Méthodologie

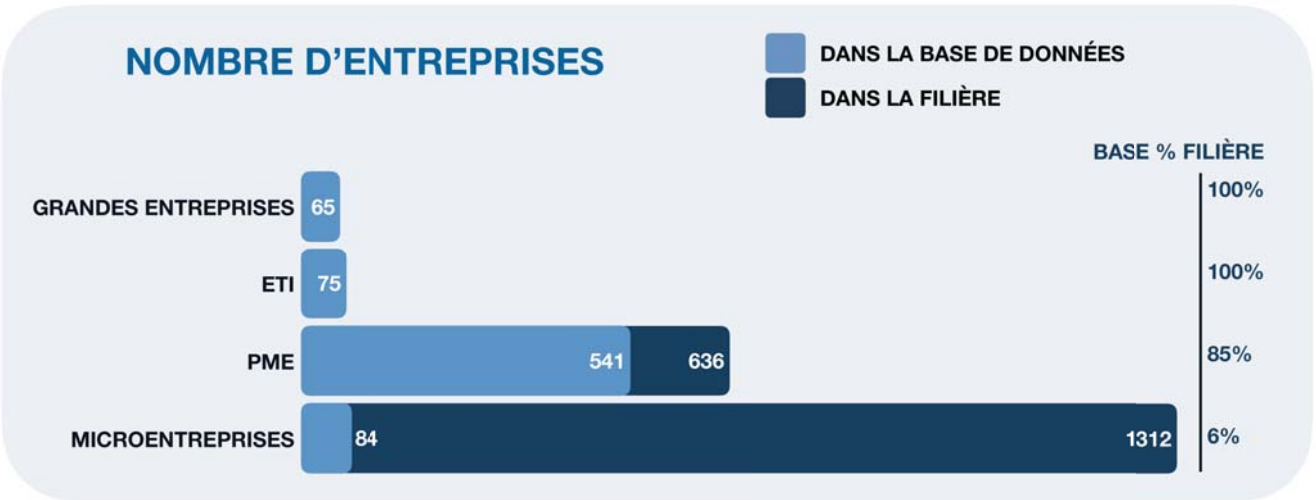
L'objectif de l'Observatoire est à la fois de définir le périmètre de la filière de la Confiance Numérique et d'en évaluer le poids économique et les caractéristiques.

Les données présentées dans ce rapport sont issues d'une base de données recensant 765 entreprises parmi les 2 088 que compte la filière de la Confiance Numérique. Cette base de données prend en compte :

- La totalité des grand groupes de la filière (65/65) ;
- La totalité des entreprises de tailles intermédiaires (ETI) de la filière (75/75) ;
- La majorité des PME de la filière (541/636) ;
- Les micro-entreprises et startups les plus remarquables et innovantes (84/1312).

Ainsi, bien que seul 37% 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 2013-2018 : 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 2018, en 2017 et en 2015.

Les chiffres sont construit sur l'année 2017 et extrapolés sur l'année 2018.

AMÉLIORATIONS PAR RAPPORT AU PRÉCÉDENT OBSERVATOIRE

- Une base de données dont le périmètre de couverture et d'analyse a augmenté de **+ 26%** (765 entreprises recensées contre 606 précédemment)
- Toutes les données présentées dans ce rapport sont mesurées et extrapolées sur la base des **765 entreprises** de notre base de données, tandis que dans le précédent observatoire la totalité des données présentées (à l'exception du chiffre d'affaires de la filière), étaient fondées sur une enquête en ligne ne recensant que **81 entreprises** de la filière de la Confiance Numérique. A l'exception du chiffre d'affaires, les chiffres présentés dans ce rapport sont donc fondés sur un nombre d'entreprises supérieur de **+ 844%** au précédent Observatoire
- Un nouvel indicateur : celui de la **valeur ajoutée**
- Une segmentation compatible avec la segmentation européenne de la filière de la sécurité dans son ensemble

En conséquence de ces améliorations, les chiffres de l'Observatoire 2019 ne sont pas directement comparables avec ceux de l'Observatoire précédent.

II) Confiance Numérique :

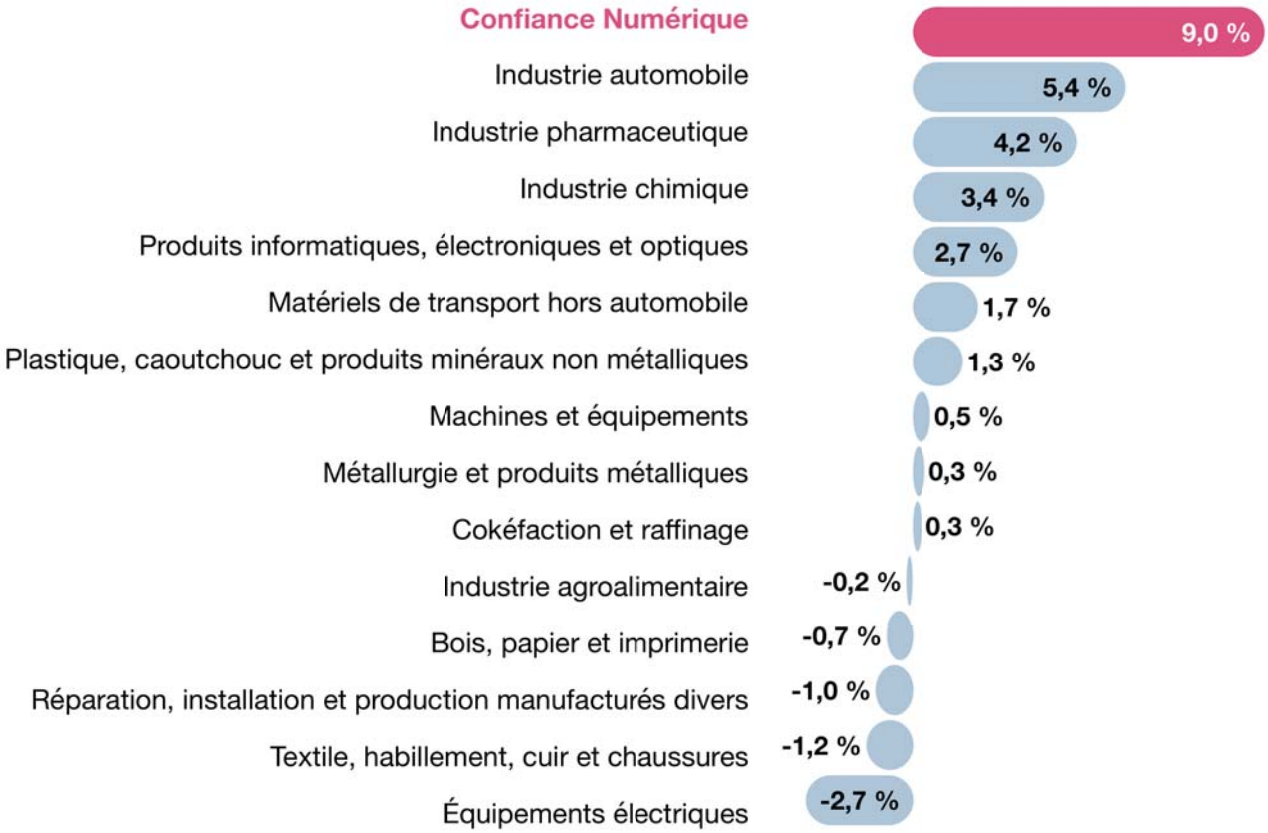
Une filière importante et dynamique

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

Sur la période 2013-2018, 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'en 2024, la Confiance Numérique devrait devenir la 11ème filière industrielle française sur 15 en valeur ajoutée en dépassant :

- La filière des équipements électriques ;
- La filière Bois, papier et imprimerie.

CROISSANCE ANNUELLE MOYENNE DES FILIÈRES FRANÇAISES SUR LA PÉRIODE 2013-2018

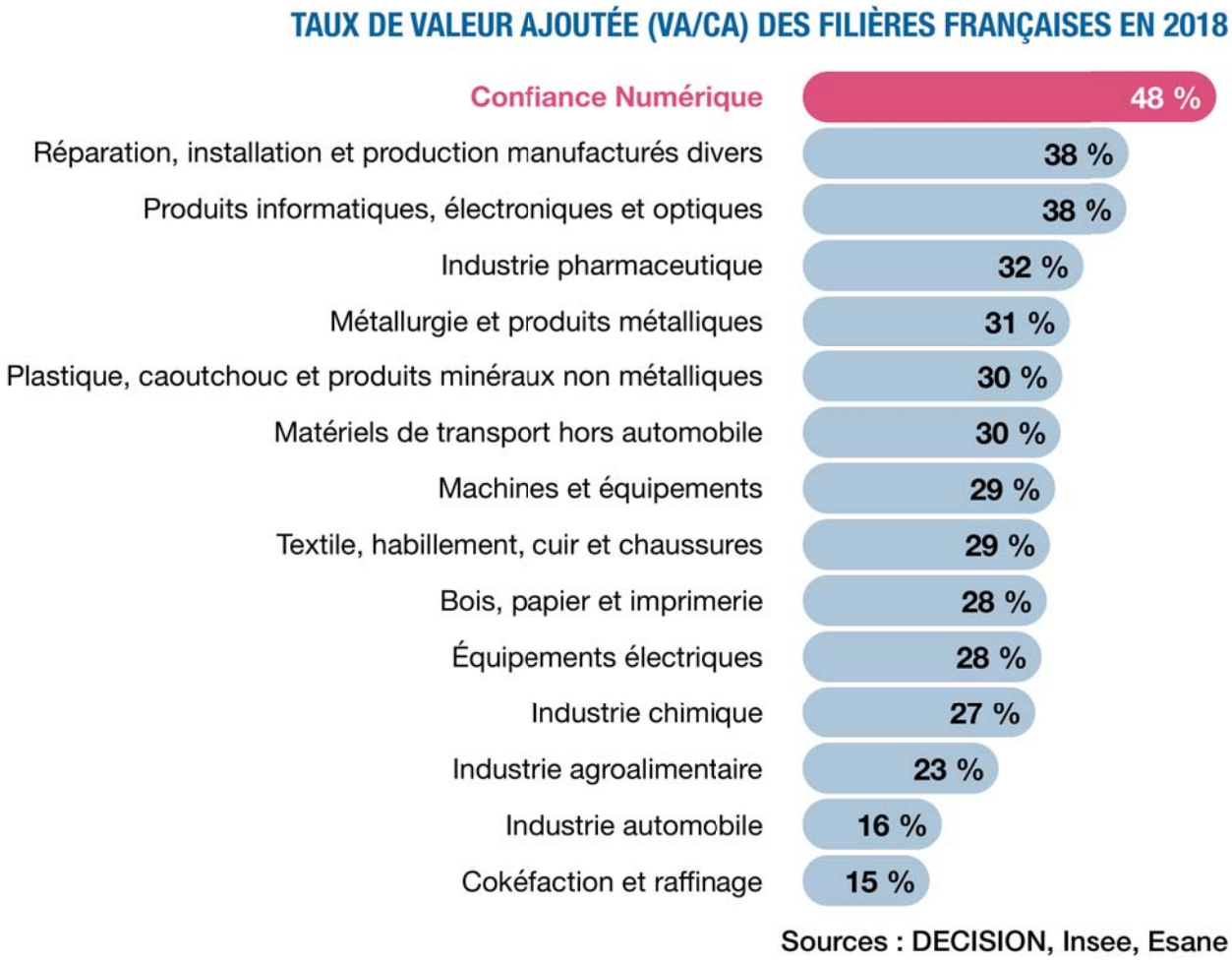


Sources : DECISION, Insee, Esane

II) Confiance Numérique :
Une filière importante et dynamique

2.2 La Confiance Numérique est la filière industrielle la plus productive

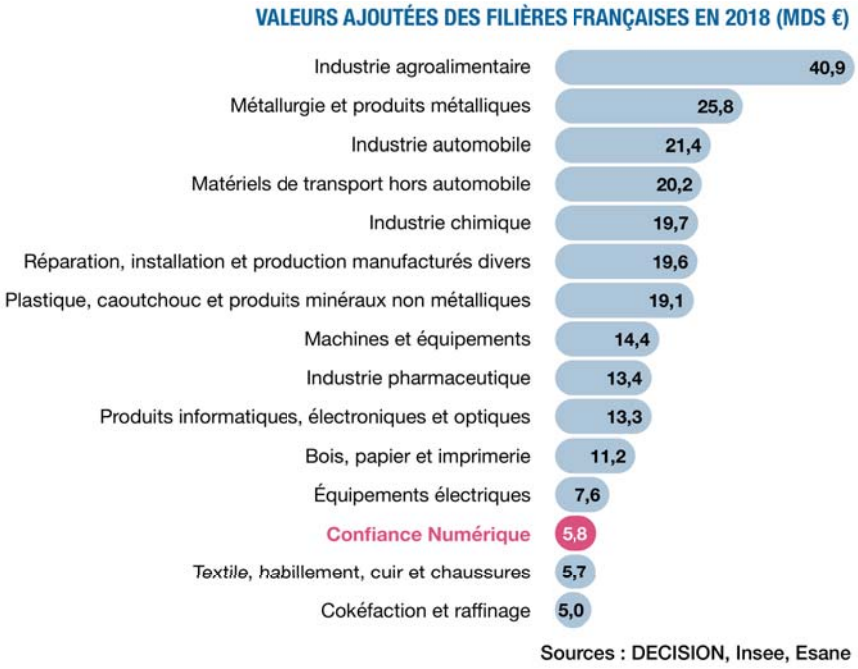
Enfin, la Confiance Numérique est de loin la filière la plus productive avec un taux de valeur ajoutée de 48% (Valeur Ajoutée / Chiffre d'affaires). En d'autres termes, la Confiance Numérique est la filière industrielle dont le degré de création de richesse, c'est-à-dire de transformation des produits au cours de l'activité est le plus élevé.



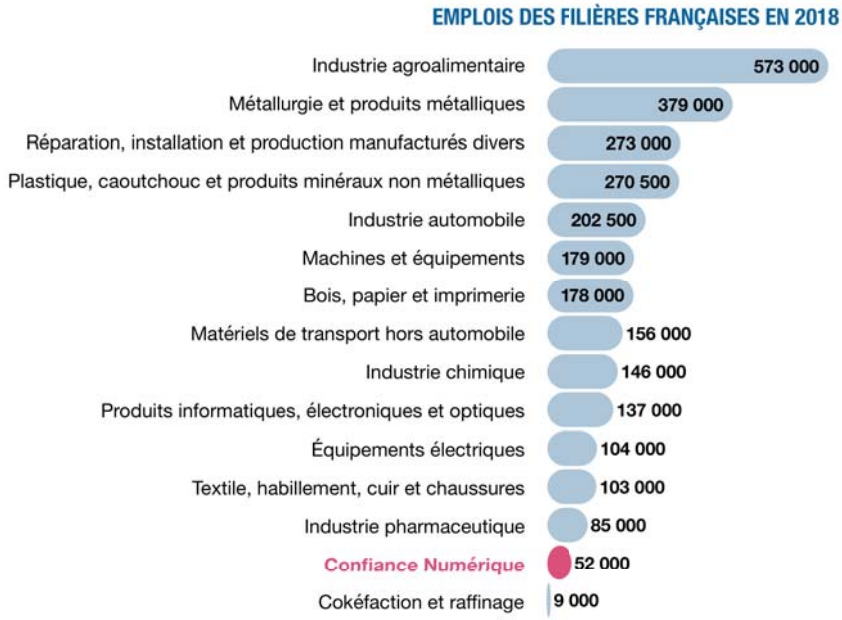
II) Confiance Numérique :
Une filière importante et dynamique

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

La Confiance Numérique est une filière industrielle à part entière. Ainsi, la valeur ajoutée totale de la Confiance Numérique était supérieure en 2018 à celle de la filière de cokéfaction et raffinage ou encore de textile, habillement, cuir et chaussures.



En termes d'emploi, la filière industrielle de sécurité dépasse largement la filière de cokéfaction et raffinage et se rapproche rapidement de l'industrie pharmaceutique ou encore de la filière de textile, cuir et chaussures.



II) Confiance Numérique :
Une filière importante et dynamique

2.4 Les acteurs français sont à la pointe 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.

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 trois facteurs, dont aucun n'est propre à la France :

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

La France bénéficie historiquement d'une filière 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 trois 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 de plus en plus forte de la part de acteurs étrangers

Les acteurs de nationalité française génèrent 78% du chiffre d'affaires de la Confiance Numérique en France, soit 9,7 milliards d'euros en 2018. Autrement dit, les acteurs étrangers de la filière réalisent 22% du chiffre d'affaires de la filière en France, soit environ 2,7 milliards d'euros en 2018. 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). Le poids des acteurs étrangers sur le marché français est estimé entre 30% et 40%.

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 2018-2024. 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 chinois ou américains.

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 2013-2018. Parmi les rachats significatifs, figure celui d'Arismore par Accenture (Etats-Unis), ou encore de DenyAll par Rohde & Schwarz Cybersecurity (Allemagne).

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 2013-2018. En effet, dans un contexte général de stagnation de la croissance (1,4%/an de croissance du PIB français sur la période 2013-2018), 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 :

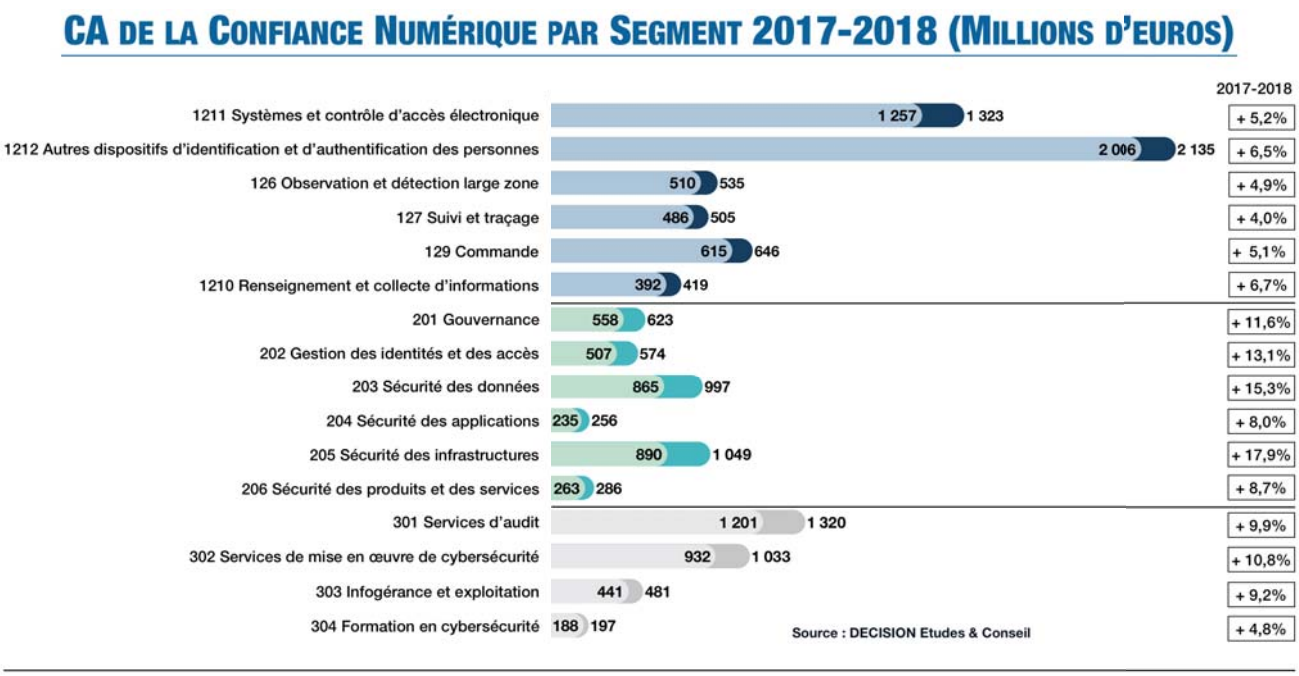
- Ce secteur est essentiel à la souveraineté numérique nationale et à l'autonomie stratégique européenne ;
- La Confiance Numérique est déjà de taille significative ;
- Les acteurs français sont à la pointe en matière de compétences et de R&D ;
- Le potentiel de croissance est durablement supérieur à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

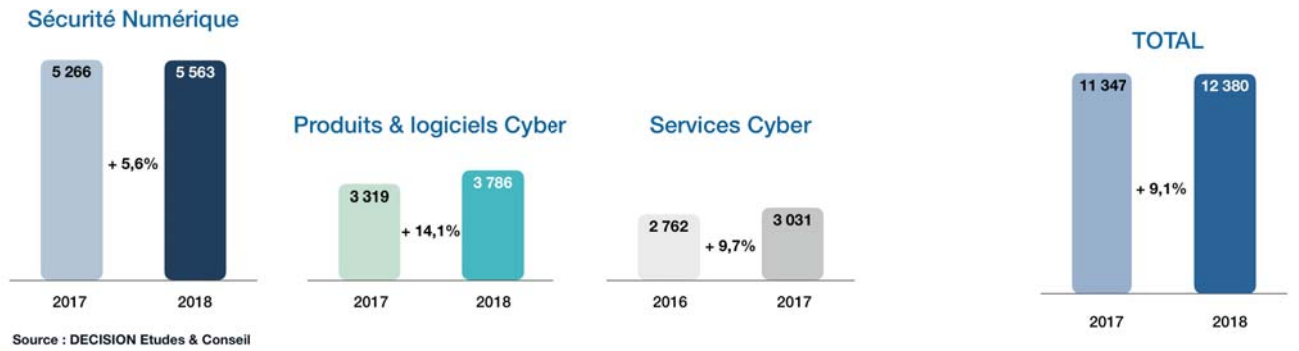
Les conditions sont réunies pour que l'effet de levier en cas de mise en place d'une politique industrielle volontariste génère un maximum de retour sur investissement, aussi bien en termes d'emploi que de valeur ajoutée sur le sol français et à l'international.

III) Les chiffres clés de la filière

3.1 Analyse par sous-segment

3.2.1 Taille et croissance 2013-2018





CA de confiance numérique en france : 12,4 Mds € en 2018

III) Les chiffres clés de la filière

3.2.2 Valeur ajoutée en 2018

VALEUR AJOUTÉE EN FRANCE EN 2018 PAR SEGMENT

SÉCURITÉ NUMÉRIQUE
2 246 M€
+
PRODUITS DE CYBERSÉCURITÉ
2 208 M€
+
SERVICES DE CYBERSÉCURITÉ
1 393 M€
=

N°	SEGMENT	VALEUR AJOUTÉE EN 2018 EN MILLIONS D'EUROS
1.2.1.1	CONTROLE D'ACCES	453
1.2.1.2	IDENTIFICATION DES PERSONNES	839
1.2.6	OBSERVATION LARGE ZONE	285
1.2.7	SUIVI - TRAÇAGE - LOCALISATION	190
1.2.9	COMMANDE - CONTRÔLE - AIDE À LA DÉCISION	299
1.2.10	RENSEIGNEMENT - COLLECTE D'INFORMATION	179
2.0.1	GOUVERNANCE	357
2.0.2	GESTION DES IDENTITÉS ET DES ACCÈS	366
2.0.3	SÉCURITÉ DES DONNÉES	601
2.0.4	SÉCURITÉ DES APPLICATIONS	177
2.0.5	SÉCURITÉ DES INFRASTRUCTURES	595
2.0.6	SÉCURITÉ DES PRODUITS & ÉQUIPEMENTS	112
3.0.1	AUDIT - PLANNING - CONSEIL	541
3.0.2	MISE EN OEUVRE CYBERSÉCURITÉ	447
3.0.3	INFOGÉRANCE - EXPLOITATION	287
3.0.4	FORMATION EN CYBERSÉCURITÉ	118

Source : DECISION Etudes & Conseil

5 850 M€ DE VA DE CONFIANCE NUMÉRIQUE EN FRANCE

III) Les chiffres clés de la filière

3.2.3 Emplois en 2018

EMPLOIS EN FRANCE EN 2018 PAR SEGMENT

SÉCURITÉ NUMÉRIQUE

22 421

+

PRODUITS DE CYBERSÉCURITÉ

15 253

+

SERVICES DE CYBERSÉCURITÉ

14 662

=

N°	SEGMENT	EMPLOIS EN 2018
1.2.1.1	CONTROLE D'ACCES	4 866
1.2.1.2	IDENTIFICATION DES PERSONNES	8 425
1.2.6	OBSERVATION LARGE ZONE	1 865
1.2.7	SUIVI - TRAÇAGE - LOCALISATION	2 127
1.2.9	COMMANDE - CONTRÔLE - AIDE À LA DÉCISION	3 410
1.2.10	RENSEIGNEMENT - COLLECTE D'INFORMATION	1 729
2.0.1	GOUVERNANCE	3 451
2.0.2	GESTION DES IDENTITÉS ET DES ACCÈS	1 863
2.0.3	SÉCURITÉ DES DONNÉES	4 324
2.0.4	SÉCURITÉ DES APPLICATIONS	899
2.0.5	SÉCURITÉ DES INFRASTRUCTURES	3 757
2.0.6	SÉCURITÉ DES PRODUITS & ÉQUIPEMENTS	959
3.0.1	AUDIT - PLANNING - CONSEIL	6 212
3.0.2	MISE EN OEUVRE CYBERSÉCURITÉ	5 411
3.0.3	INFOGÉRANCE - EXPLOITATION	2 098
3.0.4	FORMATION EN CYBERSÉCURITÉ	941

Source : DECISION Etudes & Conseil

52 300 EMPLOIS DE CONFIANCE NUMÉRIQUE EN FRANCE

III) Les chiffres clés de la filière

3.2.4 Nombre d'entreprises en 2018

NOMBRE D'ENTREPRISES EN FRANCE EN 2018 PAR SEGMENT

SÉCURITÉ NUMÉRIQUE
1 685

PRODUITS DE CYBERSÉCURITÉ
669

SERVICES DE CYBERSÉCURITÉ
664

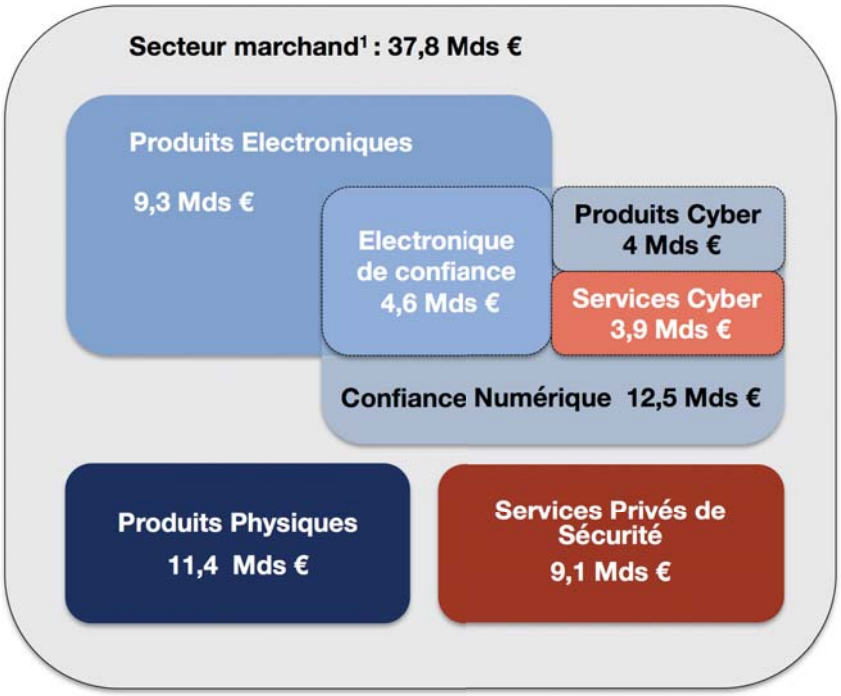
N°	SEGMENT	NOMBRE D'ENTREPRISES EN 2018
1.2.1.1	CONTROLE D'ACCES	321
1.2.1.2	IDENTIFICATION DES PERSONNES	478
1.2.6	OBSERVATION LARGE ZONE	189
1.2.7	SUIVI - TRAÇAGE - LOCALISATION	220
1.2.9	COMMANDE - CONTRÔLE - AIDE À LA DÉCISION	265
1.2.10	RENSEIGNEMENT - COLLECTE D'INFORMATION	211
2.0.1	GOUVERNANCE	197
2.0.2	GESTION DES IDENTITÉS ET DES ACCÈS	196
2.0.3	SÉCURITÉ DES DONNÉES	313
2.0.4	SÉCURITÉ DES APPLICATIONS	153
2.0.5	SÉCURITÉ DES INFRASTRUCTURES	312
2.0.6	SÉCURITÉ DES PRODUITS & ÉQUIPEMENTS	153
3.0.1	AUDIT - PLANNING - CONSEIL	660
3.0.2	MISE EN OEUVRE CYBERSÉCURITÉ	425
3.0.3	INFOGÉRANCE - EXPLOITATION	331
3.0.4	FORMATION EN CYBERSÉCURITÉ	206

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

2 088 ENTREPRISES DE CONFIANCE NUMÉRIQUE EN FRANCE

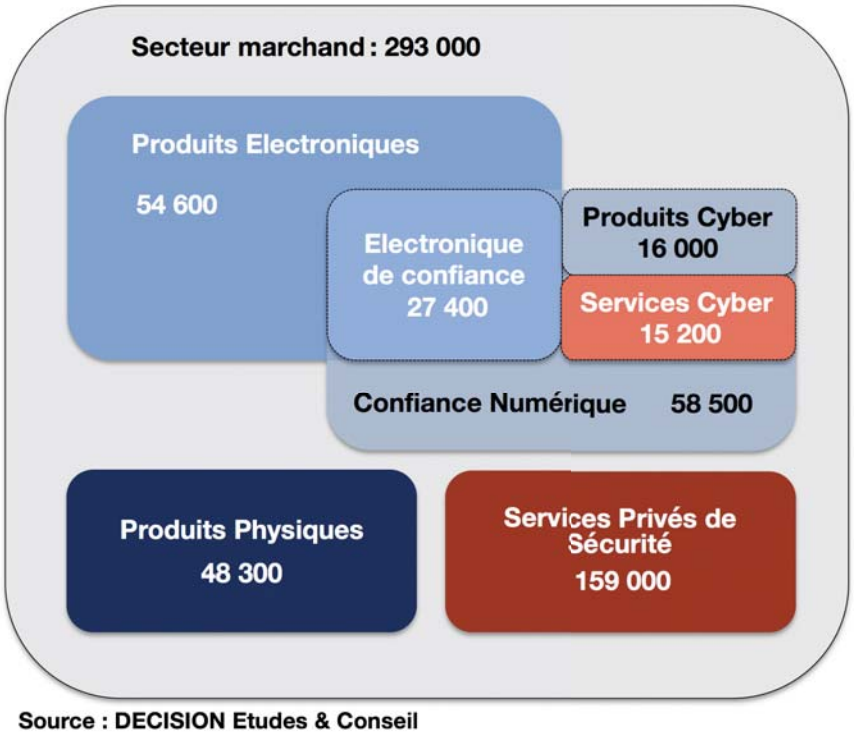
3.2 Comparaison avec les autres secteurs de la sécurité en France

CA France de la filière de sécurité en 2018



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

Emplois en France de la filière de sécurité en 2018



Source : DECISION Etudes & Conseil

IV) Les tendances de marché

4.1 Le potentiel de croissance offert par l'identité numérique

4.1.1 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.

4.1.2 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.

4.1.3 LA FRANCE, UN LEADER MONDIAL

Les acteurs français sont parmi les leaders mondiaux en matière d'identité numérique, principalement à travers Thales, Gemalto, Idemia, mais aussi à travers IN Groupe (ex Imprimerie Nationale), et Atos (notamment Atos Worldline).

En conséquence de la présence de ces leaders, le chiffre d'affaires généré en France par l'identité numérique est conséquent : 1,4 milliards d'euros en 2017, pour 5 100 emplois et une valeur ajoutée de 640 millions d'euros.

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

IV) Les tendances de marché

4.1.4 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 autre, 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 à partir de 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 2020/2021, 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 seront 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

4.2 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 désormais 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 le 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.

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

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

En effet, au niveau mondial, la croissance des industries de sécurité est portée par deux facteurs majeurs :

- **La miniaturisation couplée à la baisse des coûts des composants électroniques.**
- **La transformation digitale :**
    - Cette transformation digitale est un vecteur gigantesque de croissance pour de nouveaux logiciels dédiés à la sécurité (identification, authentification, renseignement et collecte d'information, etc.). Ce processus de digitalisation en est encore à son commencement à l'échelle mondiale. Cependant, il conduit à une croissance toujours plus importante de la part qu'occupent les logiciels dans les outils de sécurité. En particulier, les producteurs de produits électroniques – qui souffrent souvent de faibles marges – 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 ou d'Idemia- se positionnent de plus en plus fortement sur le développement de logiciels dédiés à des applications de sécurité. Les acteurs présents sur les segments physique et électronique mettent donc en œuvre de plus en plus de moyens dans le développement de logiciels de sécurité ;
    - En outre, en rendant possible l'interconnexion entre les différents réseaux de données, la transformation digitale englobe la thématique des objets connectés. En effet, plus les processus et les outils sont rendus électroniques, plus il est techniquement possible et économiquement intéressant de les interconnecter. Or, l'interconnexion génère un risque en matière de cybersécurité en rendant possible une attaque à distance. En conséquence, l'interconnexion des objets entre eux représente un potentiel de croissance gigantesque pour les produits et les services de cybersécurité. À termes, si chaque objet devient connecté, chaque objet nécessitera un outil cyber pour le sécuriser.

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. En outre, 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 en montant en gamme.

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.

4.3.2 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 2013-2017 est marquée par la fin progressive de l'achat de logiciels en mode licences et le développement de l'achat de logiciels en mode SaaS (Software as a Service), guidée par la nécessaire adaptation constante des outils de sécurité pour faire 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 toutes les entreprises de cybersécurité conçoivent la totalité de 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 conséquence est le développement progressif d'équipes internes dédiées dans chacune des unités opérationnelles chez les clients.

IV) Les tendances de marché

4.4 La prise de conscience de l'importance du Security by Design

La prise de conscience de l'importance de la cybersécurité chez les clients en France se développe depuis le début des années 2010 et commence à se généraliser en parallèle de l'augmentation des cyber-attaques motivées par des intérêts économiques de la part de hackers isolés, mais aussi d'états et d'entreprises. Ces attaques sont facilitées par la progression de la dynamique de transformation digitale : en moyenne, plus d'un tiers des données d'entreprises sont déjà stockées dans un cloud selon Gemalto. **Ces attaques sont** :

- **Plus rentables** : À cause de la création des marchés d'IoT. Les réseaux d'IoT augmentent la rentabilité des attaques car tout le réseau est touché par la cyber-attaque d'un seul objet ;

- **Moins chers** : Avec un investissement de seulement 1-2 millions d'euros, une cyber-attaque de grande envergure est désormais réalisable. A titre illustratif, la cyber-attaque de la flotte Jeep aux États-Unis en 2015 a coûté 500 000 dollars de coût de montage. Les facteurs de la baisse du coût des cyber-attaques sont les suivants :

    1. De plus en plus de possibilités d'attaque à distance sont rendues possibles. Le hacking à distance est par définition moins coûteux à mettre en œuvre qu'un hacking nécessitant une intervention physique ;

    2. Les cyber-attaques sont tolérées dans certains pays, facilitant le hacking à distance ;

    3. Le reverse engineering devient peu cher. Certaines entreprises chinoises proposent 100 000 euros pour identifier le code source des produits que leurs clients leurs envoient. Le code source permet de développer une stratégie de hacking.

L'approche « Security by design » consiste à penser la sécurité d'un produit au début dès le début de sa phase de conception.

Il y a quelques années, la majorité des clients développaient leurs produits avant de faire appel aux spécialistes de la cybersécurité. Les problématiques cyber étaient donc travaillées une fois le développement des produits achevé. Cela entrainait de lourdes pertes de temps et de moyens. Heureusement, de plus en plus d'acteurs en désormais conscience de cette problématique.

Dans cette optique, **la sécurité devient également un élément du discours marketing des clients**.

4.5 Les enjeux de la Safe City et des grands événements (JO 2024)

4.5.1 Safe City

La « Safe City » a deux composantes majeures :

- La Smart City est l'application de la tendance de transformation digitale au niveau des collectivités territoriales. Cette « Smart City », en intégrant des outils qui produisent de la donnée digitale, génère dans un second temps la problématique de la sécurisation de ces données qui est une composante majeure de la « Safe City » ;
- La seconde composante de la « Safe City » est l'ensemble des technologies numériques qui permettent d'assurer la sécurité de la ville.

Sur la période 2013-2018, la Safe City a généré une croissance importante au niveau mondial chez les acteurs de la sécurité électronique et de la cybersécurité. Les acteurs qui ont le plus bénéficié de la thématique Safe City sont les grands intégrateurs (Thales, Cap Gemini, Accenture, etc.).

La Safe City est 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 :

- La France, comme beaucoup d'autres pays européens, dispose d'une administration ancienne qui s'est construite autour de processus non digitaux. La transformation digitale de toutes ces procédures existantes est plus complexe et plus lourde que pour des pays émergents qui -n'ayant pas construit d'administrations complexes non digitalisées- peuvent sauter une étape de développement et directement mettre en place des procédures digitales en partant d'une feuille blanche ;
- La France en particulier dispose d'une grande diversité d'acteurs publics (état central, régions, départements, communes, communauté de communes, etc.) qui rend plus difficile la transformation digitale de lieux publics cogérés par plusieurs administrations indépendantes (à l'exemple de la transformation digitale d'un collège qui engage à la fois le préfet, le conseil départemental et le conseil régional) ;
- L'austérité budgétaire à l'œuvre dans les pays européens diminue les capacités financières des acteurs publics. En conséquence, les objectifs des collectivités sont souvent trop centrés sur la réduction des coûts plutôt que sur l'efficacité opérationnelle et la compétitivité de long terme.

En conséquence, les acteurs publics français se contentent encore souvent de projets de transformation digitale de faible envergure pour des budgets restreints (vidéo-protection ponctuelle, développement d'une application smartphone pour les usagers d'un service spécifique, etc.).

4.5.2 Sécurisation des grands événements (JO 2024)

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.

IV) Les tendances de marché

Ces grands évènements constituent des cibles alléchantes pour les actes malveillants et notamment les plus graves -tels des actes terroristes ou des cyber-attaques- 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…

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.

4.6 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

IV) Les tendances de marché

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.

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 2017 le marché de la sécurisation des objets connectés était encore résiduel.

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

- Le premier est l'absence de standardisation technique des architectures des IoT. Les clients potentiels qui mettent en place des réseaux d'IoT utilisent tous des objets différents avec une architecture propre, ce qui rend difficile l'application simple et immédiate des protocoles des fournisseurs des produits cyber sur ces objets.
- Le second frein est l'axe de développement actuel des objets connectés. Il semble en effet que les plateformes IoT existantes 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 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 des commandes concernant la mise en place de solution spécifiques de sécurisation d'objets connectés dans ces usines. 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.

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.

Si la croissance du marché de sécurisation des objets connectés tarde à se faire ressentir, l'unique **exception concerne les voitures connectées**. Le marché de la sécurisation des voitures connectées est devenu significatif à partir de 2015 et génère depuis une croissance de l'ordre de 7% à 10% sur la période 2013-2017. Parmi les principaux acteurs dans ce domaine, on trouve Gemalto, Idemia, Cap Gemini, Telit, Sierra wireless, etc.

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.

4.7 Matrice FFOM de la Confiance Numérique en France

Forces

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
- Des structures fédératrices dynamiques : ACN, le CSF Industries de Sécurité, les Pôles de compétitivité (SYSTEMATIC, SAFE, SCS, 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

Faiblesses

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. 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

Évènements

- Impact de l'affaire Snowden

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 2013-2018
- Structuration croissante de l'offre sécurité des entreprises
- Mise en oeuvre du RGPD
- Certification sécuritaire des objets IoT (CyberSecurity ACT)

Attitudes

- 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

Nouveaux marchés

Le phénomène mondial de transformation digitale génère en permanence de nouveaux réseaux informatiques, de nouveaux types de logiciels, de nouvelles interconnexions entre les réseaux, etc. Tous ces systèmes nécessitent d'être protégés par des outils de cybersécurité. Thèmes émergents :

- Cybersécurité industrielle et sécurité embarquée
- Sécurité de l'IOT, principalement l'automobile pour le moment
- Smart and safe city
- Analyse comportementale
- Intelligence Artificielle
- Externalisation de la Cybersécurité

Menaces

Structures

- Développement de standards américains ou autres sur les nouveaux marché

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
- 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 Capgemini et d'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

Attitudes

- Prise de conscience encore trop faible par tous les nouveaux entrants de l'importance des enjeux cyber, en particulier dans le domaine des objets connectés.

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 Entreprise, DECISION a également effectué l'étude d'évaluation du poids économique de la filière de sécurité pour le gouvernement français en 2015 (PIPAME). En 2017, DECISION conduit l'Observatoire ACN et en 2018 l'Observatoire de la filière industrielle de la Sécurité en France pour le SGDSN, le Ministère de l'Intérieur, la DGE, le CICS, Comexposium et le GICAT.

Pour plus d'informations :

www.decision.eu

DECISION
ETUDES & CONSEIL

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 · AK CYB · AMOSSYS · ARIADNEXT · Atos

business card associates · BVSTAMP · Caisse des Dépôts · Certinomis · ChamberSign · ES

LockEmail.com · DHIMYOTIS Groupe Tessi · egidium TECHNOLOGIES · ERCOM a Thales company · IDEMIA augmented identity · IN GROUPE

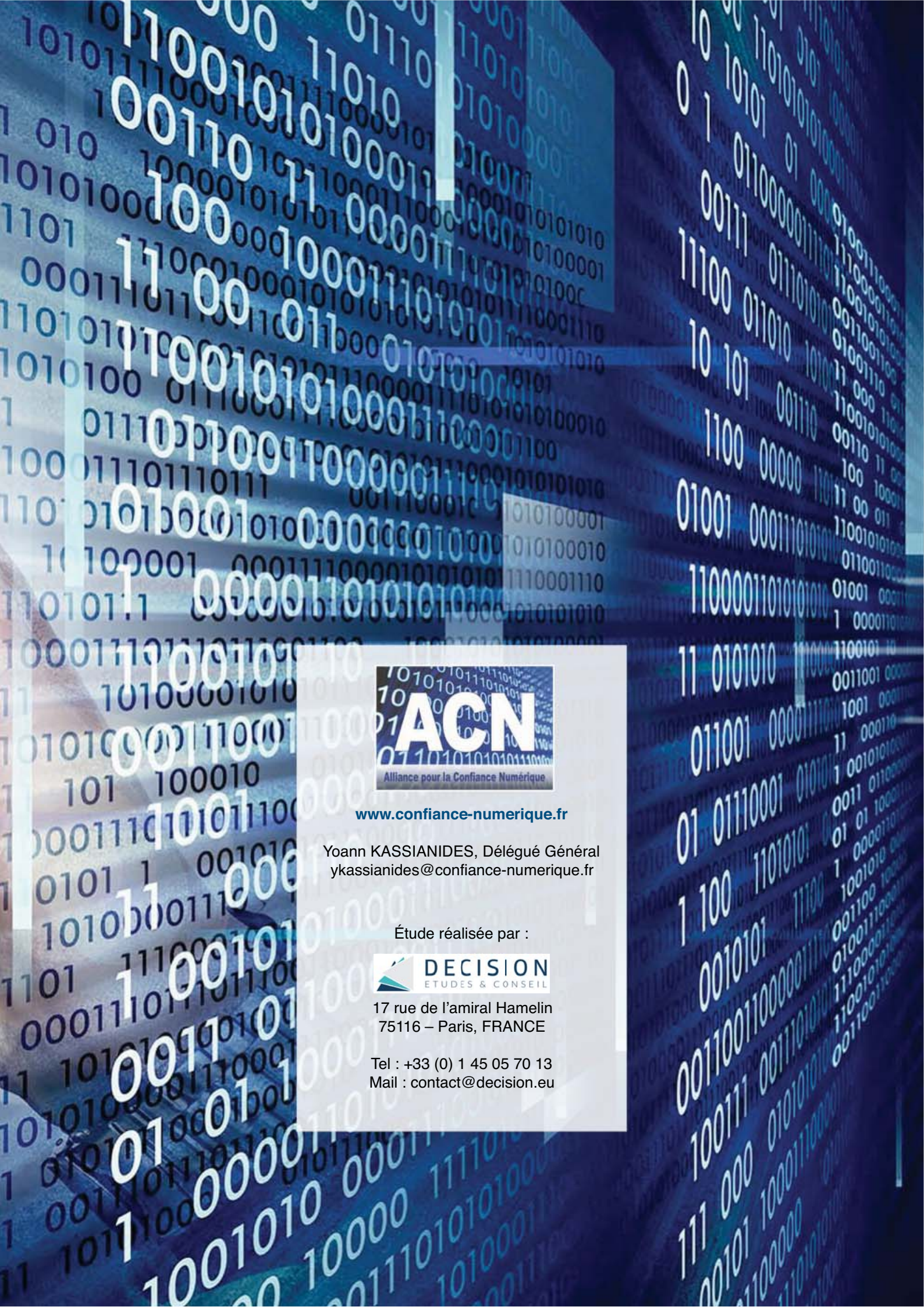
KAT · easylience · NOKIA · orange · Veliane · GUARDEA

RED ALERT LABS IoT Security · SERMA SAFETY & SECURITY · SIFARIS · Capgemini · life.augmented · SURYS

Systancia · TEHTRIS · THALES · TIXEO · YESWEHACK

Partenaires

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



ACN
Alliance pour la Confiance Numérique

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